# Theoretical Framework for Risk Factors and Safety Factors in Systems Modeling Language

A

Dissertation presented

To the faculty of the School of Engineering and Applied Science

University of Virginia

By

DeAndre A. Johnson

In Partial Fulfillment

of the requirements for the degree

**Doctor of Philosophy in Systems Engineering**

August 2024

**APPROVAL SHEET**

This
Dissertation
Is submitted in partial fulfillment of the requirements
for the degree of

Doctor of Philosophy

Author: DeAndre A. Johnson

This Dissertation has been read and approved by the examining committee:

Advisor: James H. Lambert

Committee Member: Lisa M. Colosi Peterson

Committee Member: Negin Alemazkoor

Committee Member: Venkataraman Lakshmi

Committee Member: Joi Y. Williams

Accepted for the School of Engineering and Applied Science:

Jennifer L. West, School of Engineering and Applied Science

August 2024

# ABSTRACT

This dissertation proposes a framework integrating risk management into the model-based systems engineering (MBSE) process using Systems Modeling Language (SysML). The framework describes the identification and assessment of risks while capturing comprehensive system descriptions, thus improving communication and decision-making among stakeholders. The proposed method involves designing a risk management approach that tracks risk and safety factors through SysML diagrams. These diagrams identify risk and safety factors for given systems, prioritizing system initiatives using a multi-criteria impact analysis to explore disruptions caused by emergent and future conditions. The innovative aspect of this study lies in the theoretical development of a risk management framework for SysML, which includes risk sources and safety factors, and its practical application across two examples: the supply chain for sustainable aviation fuels (SAF) and the system development of a smart parking lot systems. Applying the risk-induced framework to the SAF supply chain addresses the intricacies of blending operations attached to airport infrastructure. The methodology is subsequently extended to a smart parking lot architecture, demonstrating its adaptability and effectiveness in varied engineering scenarios. These case studies highlight the framework's ability to provide a comprehensive approach to risk management in large-scale systems and underscore its versatility in adapting to different engineering contexts. The study's findings emphasize the benefits of improved communication among stakeholders and the traceability of risk sources and controls within the SysML framework. Improved communication and semantic traceability are foundational pillars for informed decision-making, proactive risk mitigation, and the success of complex engineering projects. This research provides stakeholders with an understanding of the interplay between technical risks and administrative considerations, contributing to more effective risk management strategies and sustainable engineering solutions in diverse contexts.

# ACKNOWLEDGMENTS

The motivation for the work presented in the dissertation derives from the urge to understand how concepts learned in my Risk Analysis course taught by Professor Dr. James H. Lambert can be integrated into the growing field of MBSE. Thanks to an existing framework settled by the Center for Risk Management and Engineering Systems (CRMES) I can extend and revitalize the work and relate it to current applications. I want to thank Dr. Joi Williams and Ms. Lessie Oliver-Clark for introducing me to the opportunity to pursue a doctoral degree when I was at Virginia State University pursuing a master's in mathematics. The conversation and guidance initiated an academic expedition at the University of Virginia. I am thankful to my colleagues within the CRMES for being supportive throughout this journey to obtain a doctorate. We have collaborated on many projects, and the exhilarating experience has been meaningful and a period that I will cherish. I would like to thank the University of Virginia for sponsoring me through my educational career as a system engineer and for exposing me to many different experiences while traveling from conference to conference. I would like to thank the Commonwealth Center for Advanced Logistic Systems (CCALS), Virginia Department of Transportation (VDOT), Virginia Department of Aviation (DOAV), National Science Foundation Center for Hardware and Embedded Systems Security and Trust, and the Port of Virginia. I am grateful for the National GEM Consortium and the experience exposing me and other fellows to a coalition of black and brown Ph.D. studies within STEM across various universities, labs, and industries. I am grateful for my GEM sponsor company National Renewable Energy Laboratory taking a chance to grant an invaluable experience working with hybrid locomotive systems. This moment inspired me to press on with this Ph.D. journey. I am thankful for the exposure to academic prowess from the many IEEE, INFORMS, and SRA conferences attended in many more places. The insight that I received from researchers allowed me to establish a solid foundation for my work. I would like to thank my family for supporting me through this journey. Specifically, my siblings, fiancé, mother, and much more!

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

**ACAP**: Aviation Climate Action Plan

**ATJ**: Alcohol To Jet

**BPRIF**: Business Process Risk Integrated Framework

**CONOPS**: CONcept of OPerationS

**C-I**: Criteria Initiative Assessment

**C-S**: Criteria Scenario Assessment

**DBSE**: Document-Based Systems Engineering

**FHA**: Functional Hazard Analysis

**FMEA**: Failure Modes and Effects Analysis

**FT**: Fischer-Tropsch

**FTA**: Fault Tree Analysis

**FP**: Fast Pyrolysis

**GFT**: Gasification Fischer Tropsch

**GHG**: Greenhouse Gases

**HAZOP**: Hazard and Operability

**HEFA**: Hydroprocessed Esters and Fatty Acids

**IDEF**: Integrated Definition

**INCOSE**: International Council on Systems Engineering

**ISO**: International Organization for Standardization

**MBSE**: Model-Based Systems Engineering

**MCIA**: Multi-Criteria Impact Analysis

**OMG**: Object Management Group

**PHA**: Preliminary Hazard Analysis

**SAF**: Sustainable Aviation Fuels

**SEBoK**: Systems Engineering Body of Knowledge

**STAMP**: System-Theoretic Accident Model and Process

**STPA**: System-Theoretic Process Analysis

**SysML**: Systems Modeling Language

**UML**: Unified Modeling Language

**XMI**: XML Metadata Interchange

**XML**: eXtensible Markup Language.

# Chapter 1 | Introduction

## *1.1. Introduction*

This chapter describes the introduction in 4 sections. Section 1.2. describes the motivation for study. Section 1.3. describes the problem statement of the philosophical approach to work and introduces risk and safety factors in Systems Modeling Language (SysML) diagrams for engineering systems. Section 1.4. describes the purpose and scope of this dissertation. Section 1.5. provides an organization of the remainder of the dissertation.

## *1.2. Motivation*

Systems engineering (SE) is a critical interdisciplinary approach that enables the realization of successful systems. Early in the system development cycle, SE concentrates on identifying the needs and necessary functionality of the customer, recording requirements, and moving forward with design synthesis and system validation. This initial phase is crucial, as it sets the foundation for addressing the vast potential of severe issues that might arise later in the project lifecycle (SEBOK, 2024). Document-based systems engineering (DBSE), a methodology within SE, uses documents to capture and manage customer needs, requirements, costs, schedules, and activities throughout the system development process. DBSE ensures that knowledge is methodically organized and conveyed with precision, uniformity, and attention to detail. While DBSE provides a structured approach to information management, the increasing complexity of systems and the need for dynamic and interactive processes call for more advanced methodologies. This realization ignited the evolution towards Model-Based Systems Engineering (MBSE), which promises enhanced integration and adaptability in the face of complex project demands.

MBSE is a transformative methodology that captures and develops interconnected complex systems through digitized models. These digitized representations of the systems serve as a blueprint for the systems' virtual elements, actions, and communications, revolutionizing how systems engineers design and build processes and technology. A significant advantage of employing MBSE is the traceability across unique views and models at unique levels and abstractions (Mhenni, 2016). Traceability is highlighted by MBSE’s ability to allocate system requirements to a functional architecture. Subsequently, the functions are then allocated to the logical architecture. Finally, logical elements are then allocated to the physical architecture. Thus, this process represents how traceability through MBSE allows users to directly understand the origin of a key error or hazard (Zuken Inc., 2024). Thus, system engineers will benefit from using a digital infrastructure. A convenient way to communicate with risk analysis is a systematic process that involves understanding the nature of risk and expressing it with available knowledge (Aven, 2018). Risk management is a crucial component of risk analysis and critical evaluation.

International Standards for Systems Engineering, such as ISO-15288 and the International Council on Systems Engineering (INCOSE) Systems Engineering Handbook, explicitly emphasize the importance of risk management in the systems' life cycle processes. However, many MSBE languages, methods, and tools often relegate risk management to an afterthought (Jurewicz, 2023). As systems become more complex, developing and managing them becomes more challenging. These challenges and gaps often lead to systemic hazards and risks that are more time-consuming to identify and difficult to manage (Ericson, 2015). Therefore, integrating risk management into the system development process is crucial to ensure a systematic approach and reduce potential hazards.

Safety analysis is not just a component of systems engineering but an integral part that ensures the safety of direct users, associates, and third-party stakeholders. As the complexity and robustness of system safety increases, so does the potential severity of accidents, making it essential to address safety concerns early in the system development process (Vincoli, 2024). Identifying safety requirements at conception is beneficial and essential for achieving the expected design outcomes. Consequently, safety analysis must not just be woven into every phase of system development but be a proactive measure to ensure comprehensive integration (Chasson, 2022). A notable challenge within the design process is the miscommunication between safety analysts and systems engineers, which can hinder the consideration of safety factors at an early stage. Addressing the communication gap is not just crucial but a responsibility; overlooking it can lead to significant cost and safety oversights.

Assessing the safety of a system's design involves industry experts, systems engineers, and risk and safety analysts. According to an INCOSE study, identifying and eliminating design faults during the design phase is significantly more cost-effective than at later stages. Specifically, addressing these issues during the design phases is six times less costly than during the concept phase (Wan, 2023).

Moreover, the cost increases dramatically, by 100 and 1000 factors, when faults are detected during the development, production, or testing phases (Haskins, 2007; Baklouti, 2019). These significant cost increases emphasize the importance of conducting early and thorough safety risk assessments. However, the financial implications alone do not solely drive this imperative. The interaction between humans and systems further accentuates the need to seamlessly embed risk and safety evaluation within MBSE, ensuring that safety is an integral and proactive component of the system development lifecycle.  The relationship between the three disciplines

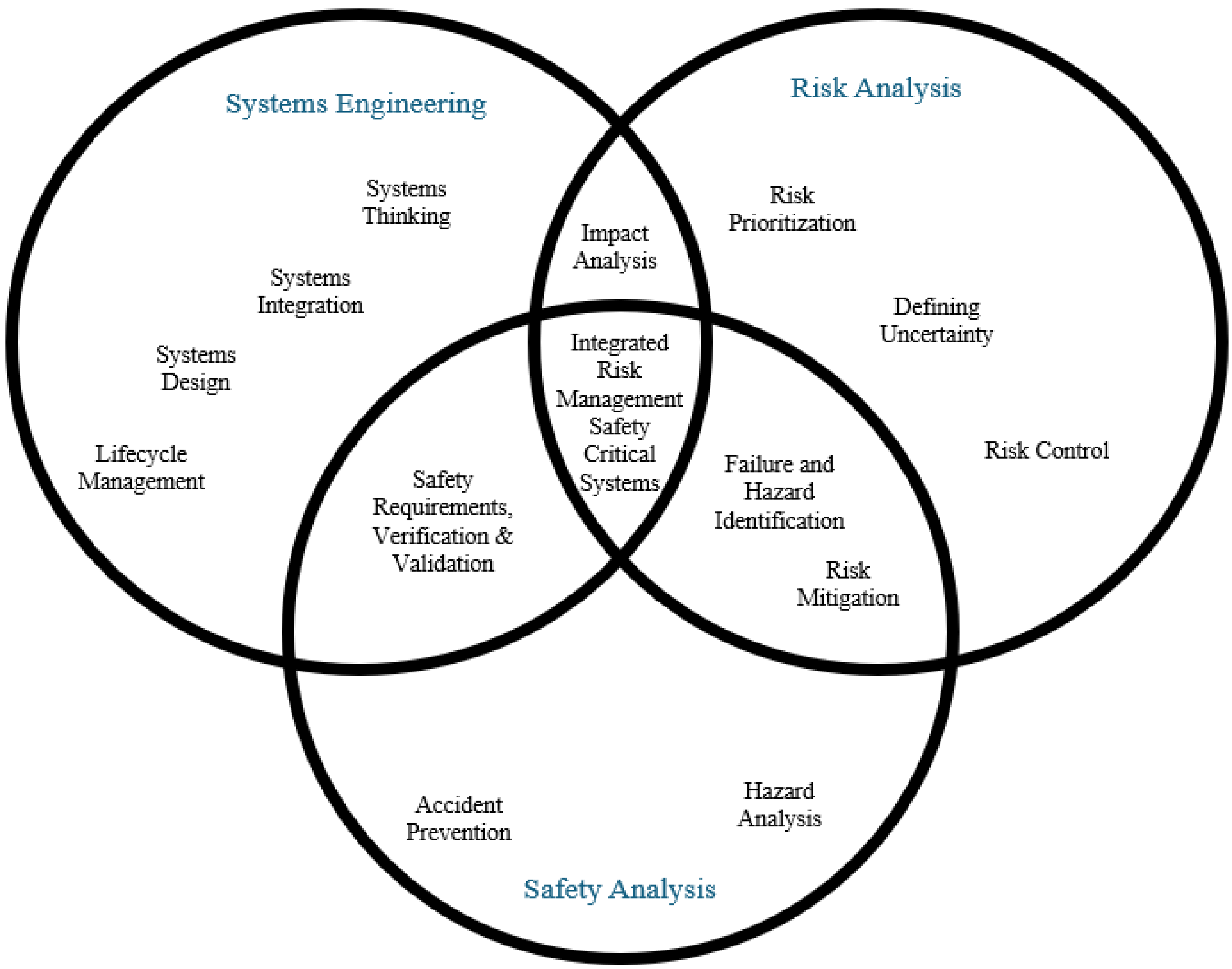



**FIGURE 1. Venn Diagram representing the relationship among Systems Engineering, Risk Analysis, and Safety analysis in complex systems.**

sheds light on the potential benefits of their integration while leveraging the unique abilities that each displays. Integrating the unique strengths of each discipline allows users to craft a holistic approach to integrated risk management for safety-critical systems. This approach evaluates the multi-dimensional aspects of safety, risk, and systems engineering, enhancing the robustness and reliability of critical systems.

Stakeholders of various disciplines in a project communication are critical, but it is difficult to challenge transitioning from document-centric SE to MBSE. Additionally, many modeling languages for systems do not offer the possibility of creating risks and errors to determine impact across departments (Kunnen, 2019). Furthermore, the separation of methods, MBSE, and risk and safety analysis affect the ability of stakeholders to identify early project issues within the developmental phase (Uludag, 2022). Risk and safety analysis must be integrated into MBSE to address many challenges and streamline risk factors and safety factors identification. By adopting risk management techniques, stakeholders can anticipate the impact of risks on a particular activity and implement risk treatment for the hazards.

## *1.3. Problem Statement*

In the realm of complex systems development, where diverse disciplines converge, there exists a critical gap in effectively communicating and managing project risks throughout the lifecycle of a project. Current tools and methodologies in Model-Based System Engineering (MBSE), particularly those utilizing SysML (Shevchenko,2020), excel in delineating technical roles and responsibilities. However, they must catch up in risk and safety management aspects. Traditionally, safety and risk analysis techniques have been employed independently, causing engineers to be prone to mistakes and needing more global consistency and continuity between safety and risk models for MBSE tools. This inadequacy hinders the transparent and traceable communication of potential risks to various stakeholders involved, posing a significant challenge in ensuring the successful execution and delivery of multifaceted projects—SysML's ability to create extensions (model components not included in SysML).

The absence of a robust mechanism to integrate risk management within MBSE frameworks leads to disjointed risk perception, potentially resulting in overlooked vulnerabilities, mismanaged priorities, and unaligned decision-making processes. Consequently, projects need more comprehensive risk visibility and accountability, facilitating their integrity and success. Therefore, developing an integrated approach that embeds risk management within the MBSE process utilizing SysML is imperative. This integration should facilitate the seamless traceability of risks, enhance the clarity and accessibility of risk-related information for all stakeholders, and support continuous, dynamic risk assessment and mitigation throughout the project lifecycle. Such an advancement in MBSE methodologies will bridge the risk and safety communication gap and bolster the resilience and adaptability of complex systems development in an ever-evolving multidisciplinary landscape.

## *1.4. Purpose and Scope*

Adopting MBSE across industries has contributed to abandoning traditional document-based system engineering. The challenges and gaps in current MBSE practices are mentioned in the precedent section. This dissertation aims to introduce a framework that supports risk and safety analysis using MBSE, namely SysML models. This study proposes enhancing the means to address risk and safety to better understand complex systems through system modeling introduced by the System Engineering Body of Knowledge (SEBoK). The innovative approach of this method is a combination of efforts, such as the visual design of how risk and safety are emulated in the SysML model and the application of a multi-criteria impact analysis.

The methodological approach will apply across industries that use MBSE to deploy risk and safety assessments for systems within the early conception phase. The study proposes to validate and verify the framework's effectiveness by comparing state-of-the-art practices and traditional approaches while providing explicit expert feedback. The study combines risk analysis, model-based systems engineering, and safety analysis.

## *1.5. Organization of Dissertation*

The structure of this dissertation is shown in Table 1. Chapter 2 establishes the literature review for system engineering aspects such as MBSE, risk analysis, and safety analysis. Chapter 3 describes the methods for conducting a multi-criteria impact analysis for SysML models. Chapters 4 -5 describe using the multi-criteria impact analysis on two cases. The first case involves establishing an intelligent parking lot for a generic smart city. The second case establishes the context for strategizing supply chain techniques for sustainable aviation fuels deployed at various locations such as airports and refineries. Chapter 6 summarizes the best practices for integrating risk and safety factors for SysML diagrams and prioritizing initiatives. Chapter 7 describes how previous benchmark methods will be implemented in various cases. Chapter 8 summarizes the study's contributions, future directions for this research, and a conclusion. The dissertation ends with references and an appendix.

**TABLE 1. Overview of Dissertation Structure for Extending SysML Diagrams with Safety and Risk Factors.**

| CHAPTER | TITLE | DESCRIPTION |
|---|---|---|
| 1 | Introduction | Overview of motivation, problem statement purpose, scope of the work, and dissertation organization. |
| 2 | Literature Review | Literature review for risk analysis and management in Systems Engineering, MBSE, Risk as Supporting Aspect of MBSE, Identifying gaps in the practice. |
| 3 | Theory and Technical Approach | This task outlines the development of a theoretical framework and technical methodology, introduces SysML and its diagrams, and demonstrates their application through a case study. It is organized into three subsections and incorporates risk management and multi-criteria analysis for system safety validation and risk-based decision-making. |
| 4 | Case Study 1: Smart Parking Lot System | This task outlines the implementation of risk integration into SysML Diagrams and proposes the multi-criteria impact analysis of the Smart Parking Lot System. |
| 5 | Case Study 2: Supply Chain for Sustainable Aviation Fuels | This task outlines the implementation of risk integration into Activity Diagrams SysML and proposes the multi-criteria impact analysis for the Supply Chain for Sustainable Aviation Fuels. |
| 6 | Synthesizing Best Practices and Advancement in Extending Risk Factors and Safety Factors in SysML | This section will distill the key practices that led to successful outcomes based on the methodology applied to the cases. It will elaborate on how these best practices can be generalized or adapted to another context within the field. |
| 7 | Comparative Analysis | This section then provides previous benchmark methodologies. This will then establish the criteria for comparing the methods. |
| 8 | Conclusion | Outlines the study's current contribution while recognizing existing and future publications. |

# Chapter 2 | Literature Review

## *2.1. Introduction*

This chapter describes the literature review in five sub-sections. Section 2.2 describes the use of MBSE and its role in SE. Section 2.3 describes existing risk analysis and risk management within systems engineers. Section 2.4 describes existing risk, safety analysis, and safety management frameworks within systems engineering. Section 2.5 is a literature review of previous practices of integrating risk and safety as supporting aspects of MBSE. Section 2.6 highlights the gaps from previous studies and the proposed framework for this methodology. Section 2.7 is a summary of the chapter's contribution to discipline between safety, risk, and systems engineering.

## *2.2. Model-Based Systems Engineering*

MBSE is defined by INCOSE as the formalized application of modeling to support system requirement, design, analysis, verification, and validation, beginning in the conceptual design phase and continuing throughout the development and later life cycle phase (Handerson & Salado, 2021). MBSE represents a sophisticated tier within systems engineering designed to tackle complex problems. MBSE addresses complexity, enhances communication among stakeholders, boosts quality and productivity, and mitigates risks (Krasner, 2015; Carroll, 2016; Patou, 2018). The motivation for using MBSE is to overcome deficiencies and undesirable practices related to the system's architecture and design. Organizations often begin modeling without realizing that the original goal may be replaced with a narrow, defined solution that abandons unnecessary expenses. Thus, system architecture is an essential aspect of MBSE that warrants meticulous focus (Madni, 2018).

The growing complexity of systems has made the management of DBSE difficult due to the excessive time spent managing information. MBSE simplifies complex systems by collecting and presenting critical information. MBSE's ability to relay information relevant to systems requirements, design, and analysis and to trace changes throughout the development process represents a significant advantage over traditional DBSE. The models in MBSE serve as primary artifacts for processes within systems engineering, including methodical and illustrative models applicable down to the component level. SysML, an all-purpose graphical modeling language under MBSE, is used to develop technical systems. It is regarded as the successor of UML, primarily focusing on software-specific development. SysML captures requirements, behaviors, structure, and parametric data through a new set of diagrams and modifications of existing UML diagrams. Figure 2 highlights the hierarchy of SysML diagrams, showing the Behavior Diagrams, Requirements Diagrams, and Parametric Diagrams, with requirements and parametric diagrams being new additions.

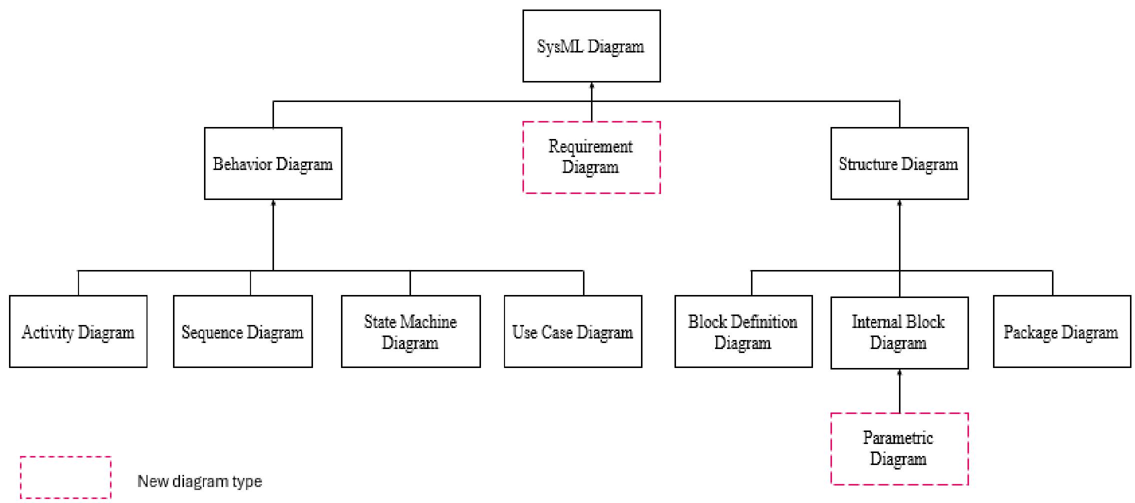



**FIGURE 2. Taxonomy of SysML diagrams taken from (OMG, 2018).**

Over the years, numerous initiatives have integrated MBSE across various applications, significantly contributing to its evolution. The journey began in 1993 with Wymore's foundational expression of MBSE, leading to the development of Integrated Definition (IDEF) models and the more sophisticated Systems Modeling Language (SysML) models, reflecting MBSE's expanding role in systems engineering and design.

## *2.3. Risk Management within Systems Engineering*

System engineering societies have significantly enriched the knowledge framework by advancing our understanding of risk analysis as a management concept. The SEBoK is a system engineering handbook that allows system engineers to employ best practices and methodologies for risk management. SEBoK's glossary defines risk as the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints. It has two components: The probability (likelihood) of failing to achieve a particular outcome and its consequences (impact). Likelihood and impact are quantitative metrics used to produce an output to quantify the severity of a system's risk.

The SEBoK defines risk management as the organized process for identifying and handling risk factors (ISO/IEC/IEEE 2010) (SEBOK, 2023). Within the systems engineering domain, the application of risk analysis is iterated throughout a project to identify risk, quantify the level of risk, and evaluate the impact and severity of the risk to determine the negative or positive deviation from the project's expected goals. MITRE, 2014) is a non-profit organization that focuses on providing technical guidance to complex engineering challenges for various U.S government projects, established a common risk management framework for systems engineers by defining risk management: identifying risk, assessing risk, and taking steps toward mitigating risk (Stoneburner, 2002).

Figure 3 describes the risk management framework, including risk identification, which describes internal and external risk collection for engineering systems projects.

- Risk Identification: Collecting internal and external risks relevant to engineering systems projects.
- Risk Impact Assessment: Evaluating the consequences of identified risks.
- Risk Prioritization Analysis: Ordering and ranking risks from least to greatest and allocating resources accordingly.
- Risk Planning: Designing control strategies to mitigate, prevent, and minimize risks.

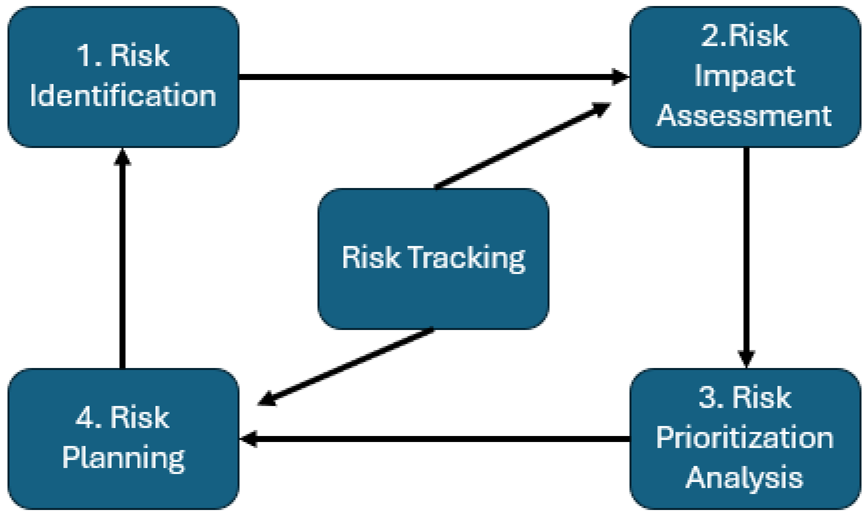



**FIGURE 3. Fundamentals of risk management adapted from (MITRE Corporation, 2014).**

In systems engineering, risk analysis involves examining how system outcomes and objectives might change due to the impact of risk events. Numerous studies have applied risk analysis to understand how different scenarios can influence these impacts (Moghadasi et al., 2023; Marcellin et al., 2023; Baker, 2023). Various methods are used to conduct risk analysis for complex systems. One such method is the Hazard and Operability (HAZOP) study, a qualitative risk procedure designed to identify how a process may deviate from its intended design. The HAZOP process involves a detailed examination of the process and equipment, typically conducted by a risk manager, to track how deviations occur and determine the potential consequences (Harahap, 2024).

## *2.4. Safety Management within Systems Engineering*

While risk management is essential, it should not overshadow the critical role of safety management in complex systems. Safety management significantly contributes to the design of safety-critical systems, enhancing human and system performance. A safe system undergoes thorough safety analysis starting in the conceptual phase and continuing throughout the development and acquisition life cycle (Ericson, 2011). *Safety engineering* is defined as managing complexity while avoiding conditions that could cause death, injury, illness, damage to or loss of equipment, and environmental harm (Sojka, 2024).

Safety engineering is crucial in developing complex systems by focusing on human and system performance. The primary objective of safety engineers is to integrate safety-related requirements into system designs (Buede & Miller, 2024). Safety analysis techniques derived from national safety standards, such as ISO 26262 and IEC 61508, are employed to ensure the safety of these complex systems. For instance:

- Preliminary Hazard Analysis (PHA): This process identifies potential hazards, causal indicators, risks, and control strategies to enhance system safety (Hadj-Mabrouk, 2017; Xin et al., 2023). It is essential because it allows engineers to proactively identify and mitigate potential hazards early in the design process, reducing the likelihood of accidents or failures during system operation.
- Functional Hazard Analysis (FHA) is a structured method for evaluating potential causes and hazardous consequences of functional failures within a system (Tran, 2021). FHA ensures a comprehensive analysis of system functions, minimizing the risk of functional failures that could compromise safety.
- Failure Modes and Effects Analysis (FMEA): Offers a reliable framework for identifying and mitigating potential issues and failures within a system before they occur (Press, 2018). FMEA enables engineers to systematically identify failure modes, assess their potential effects, and implement appropriate mitigation measures, enhancing system reliability and safety.

- Fault Tree Analysis (FTA): This technique serves as a standard safety analysis practice applied to various complex systems, aiding in identifying potential failure pathways (Liu, 2024; Wijayaningtyas, 2024). FTA is critical for understanding interdependencies between system components and identifying critical failure scenarios, allowing engineers to prioritize safety-critical elements and allocate resources effectively. These safety analysis techniques collectively contribute to the robustness and reliability of complex systems, ensuring safe operation in various domains and minimizing the risk of catastrophic failures.

(Provab, 2020) proposes that safety management can be described in two distinct modes: centralized control and guided adaptability. Centralized control aims to align and control the organization and its people by determining what is safe. In contrast, safety management through guided adaptability aims to enable the organization and its people to adapt to emergent situations and conditions safely. Adopting a system perspective for safety analysis is highlighted using the Systems-Theoretic Accident Model and Process (STAMP) approach, which considers the complexity and interdependence within systems. STAMP provides comprehensive insights into addressing potential safety challenges while creating solutions for technical, organizational, and human interventions (Zhang et al., 2022).

## *2.5. Risk and Safety as a Supporting Aspect of Model-Based Systems Engineering*

According to SEBoK (Hutchinson, 2023), an interacting combination of system elements characterizes systems that accomplish a defined objective. System engineers tend to characterize systems as models (Friedenthal, 2023) to abstract significant attributes of a system within the conceptual phase. There is a need to integrate risk into system models due to the inevitable risk from other systems or the environment threatening a system objective. Therefore, various studies contribute to integrating risk into system models, such as Lamine et al. (2020) introducing the Business Process Risk Integrated Framework (BPRIF) and a tool called adoBPRIM, which addresses the need for more foundations dedicated to the tool. The studies conducted by Johnson (2022; 2023) employ risk identification as an extension to integrated definition models IDEF 1 and 2. The objective was to enhance the process model by offering a comprehensive approach to tracking risk identification, thereby improving the system model's capacity to communicate risk information effectively to various stakeholders

Incorporating insights from Kunnen (2019), the study underscores the importance of integrating errors and risk within system models to establish connections with requirements or other system elements. This integration facilitates cross-structural traceability and aids in identifying the root cause of errors. The study reveals that best practices rely on creating errors and risks within the model and linking them to components, requirements, and other systems, enabling cross-structural traceability, which helps determine the influences of error in an event. Clegg (2019) utilizes a profile attribute to extend SysML for Failure Modes and Fault Trees. Uludag (2023) proposes a comprehensive SysML profile designated for risk management that encompasses interconnected safety analysis adapted from FMEA, FTA, and FHA. Adaptability is valuable in complex systems where multiple facets of safety and risk analysis are necessary for a comprehensive risk assessment.

Biggs et al. (2018) rely on existing ISO and IEC standards and do not enforce a new approach to safety and reliability. The profile aims to provide a foundation for the model-based treatment of safety and reliability. Biggs et al. (2019) note that safety is a supporting aspect of system models. The Object Management Group (OMG) proposes a method that uses existing

SysML to automate safety and reliability tasks with current modeling tools, thereby enhancing efficiency and consistency in the analysis process. For instance, the 2019 study introduces an Integrated System Design and Safety (ISDS) framework that integrates traditional safety analysis techniques with an MBSE design approach for the entire system lifecycle. The ISDS framework includes customizing existing SysML Block Diagrams by extending stereotypes to represent safety-related information. Safety includes goals, failure modes, and hazards (Krishnan, 2020). Krisnand (2019) uses safety-related information to perform a sub-system hazard and risk assessment (FTA) system. The benefit of this study includes the ability to automatically retain the safety-related information from a custom SysML diagram to create an FMEA. A study titled "Enhancement of FMEA risk assessment with SysML" synthesizes a safety and risk assessment method within MBSE to inform rail organizations of how technological changes impact safety. The study generates a use case diagram as a set of scenarios to define the system context that must be analyzed. (Shirvani et al., 2019) describe scenarios in their study and introduce their innovation of enhancing risk management by incorporating it into activity diagrams to illustrate how failure modes can be linked to the processes in which they may occur. The study continues to conduct a risk assessment using the activity diagram to demonstrate an impact analysis of a failure mode of a process. The study offers many benefits, such as automatically updating risk tables to reduce transcript errors and enabling SysML diagrams to track information that will improve system inefficiencies.

De Souza's (2020) study proposes combining Systems-Theoretic Process Analysis (STPA) and SysML modeling activity. STPA, based on the STAMP methodology, identifies hazardous control actions, loss scenarios, and safety requirements within systems. Combining STPA with SysML makes it possible to verify system models formally. This formal verification ensures system requirements are met and identifies potential hazards or safety concerns early in development. The method tackles the challenges in safety-critical systems by leveraging the strengths of safety assessment and the systems engineering approach of SysML.

**TABLE 2. Synthesis of the contribution from various studies towards integrating risk into the system model, offering a clear view of the advancements, methodologies, and key findings in this area.**

| Authors | Year | Study Focus | Methodology | Key Findings | Contributions to System Models & Risk Integration |
|---|---|---|---|---|---|
| ***Hutchinson*** | 2023 | System characterization | Conceptual analysis | Systems as interacting elements for defined objectives | Highlighted the complexity and interaction within systems, underpinning the need for risk integration. |
| ***Friedenthal*** | *2023* | System representation through models | Theoretical discussion | Models simplify systems for a better understanding | Stressed the importance of models in understanding and managing systems, providing a foundation for integrating risk. |
| ***Lamine et al.*** | 2020 | Business Process Risk Integrated Framework (BPRIF) | Development of BPRIF and adoBPRIM tool | Addressed foundation needs for risk integration tools | Developed a framework and tool for integrating risk into business process models, enhancing risk management capabilities. |
| ***Johnson*** | 2022 | Risk Identification in IDEF models. | Extension of IDEF models. | Enhanced process models with risk identification | Improved the system model's ability to communicate risk, facilitating better |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | stakeholder understanding. |
| ***Johnson*** | 2023 | Continuation of risk integration in IDEF Models. | Further extension of IDEF models. | A comprehensive approach to tracking risk | Enhanced communication of risk information through improved model processes. |
| ***Kunnen*** | 2019 | Error and risk integration within system models | Conceptual and theoretical analysis. | Linking errors and risks to system elements for traceability. | Highlighted the need for cross-structural traceability in models to identify and manage risks and errors. |
| ***Clegg*** | 2019 | Extending SysML for failure modes and fault trees | Development of SysML profile attributes | Enhanced SysML with failure modes and fault trees | Enabled more detailed safety and risk analysis within system models through extended SysML attributes. |
| ***Uludag*** | 2023 | Comprehensive risk management SysML profile. | Development of SysML profile for risk management | Comprehensive SysML profile for interconnected safety analysis | Provided a robust framework for risk management within complex systems, incorporating various safety analysis techniques. |
| ***Biggs et al.*** | 2019 | Automation of safety tasks in SysML. | Integrated System Design and Safety (ISDS) framework | Automated safety and reliability tasks in system modeling | Leveraged SysML to enhance efficiency and consistency in safety analysis, contributing to the lifecycle management of systems. |
| ***Krishnan*** | 2020 | Safety in system models. | Customization of SysML Block Diagrams | Representation of safety-related information in models | Enabled sub-system hazard and risk assessment through customized SysML diagrams, improving safety analysis. |

| | | | | | |
|---|---|---|---|---|---|
| ***Shirvani et al.*** | 2019 | FMEA risk assessment enhancement with SysML. | Use case and activity diagrams for risk assessment | Enhanced risk management in activity diagrams | Offered innovations in risk assessment within SysML, improving the accuracy and efficiency of safety analysis. |
| ***De Souza*** | 2020 | Combining STPA with SysML modeling. | Integration of STPA and SysML | Formal verification of system models with STPA and SysML | Addressed safety critical systems challenges by merging safety assessment techniques with SysML, enhancing early hazard identification and system verification. |

## *2.6. Gaps within the practice*

Existing studies demonstrated the integration of risk in system models, whether through business process models such as IDEF or MBSE tools such as SysML. However, it is crucial to acknowledge specific gaps and limitations inherent in these approaches. One notable limitation is the inability to systematically track risk for all system models and reproduce models adaptable to the system environment. Additionally, there is a challenge in reproducing models that are adaptable to system models. Existing practices cannot prioritize the system order of requirement, case, etc., within system models based on the success criteria amongst disruptive scenarios. Moreover, the current framework has yet to integrate the identification of control factors into the system. The current gap hinders the establishment of effective control mechanisms to mitigate identified risks.

Furthermore, previous studies have yet to elicit stakeholders to capture system risk and control; therefore, there is a need for an interdisciplinary approach to understanding the methods.

Additionally, managing the complexity inherent in system models when integrating risk poses a significant challenge. Complex systems often involve numerous interconnected components and interactions, making identifying and tracking risks difficult. Using strategic methodologies for simplifying and managing this complexity could improve the scalability and usability of risk integration frameworks.

Moreover, system models must incorporate dynamic risk assessment capabilities. Systems operate in dynamic environments where risks evolve due to changes in technology, regulations, or external factors. Augmenting existing frameworks to enable real-time or continuous risk assessment would allow organizations to adapt to emerging risks and threats. Decision support mechanisms should be embedded within risk integration frameworks to provide actionable insights to decision-makers. These mechanisms help decision-makers make informed decisions about risk mitigation strategies and resource allocation. Integrating decision support tools or algorithms within system models facilitates risk-informed decision-making processes.

Furthermore, aligning risk management practices with system lifecycle management processes is essential. Risk identification, assessment, and mitigation should seamlessly integrate into system development, deployment, and operation phases. Aligning risk integration frameworks with established lifecycle management methodologies ensures comprehensive risk management throughout the system lifecycle. Validation and verification of risk-integrated system models are critical to ensuring their accuracy, reliability, and trustworthiness.

Researchers should explore methodologies or techniques for validating risk models and verifying compliance with relevant standards or regulations. Lastly, education and training initiatives must build stakeholders' awareness and competence in risk integration practices. Collaboration and shared understanding among diverse stakeholders are essential for effective risk management. Strategies should be implemented to promote knowledge sharing, capacity building, and skill development in risk integration methodologies and tools. In conclusion, while existing studies have made valuable contributions to integrating risk into system models, addressing these gaps and challenges can significantly enhance the effectiveness and applicability of existing frameworks.

## *2.7. Summary*

This section highlights Chapter 2's contributions. Chapter 2 describes the basis for utilizing MBSE within SE. This chapter highlights existing frameworks within SE that use risk management for complex systems. The chapter introduces literature on safety management within SE for complex systems. The chapter then reviews the literature to emphasize other authors' contributions to progress risk and safety within MBSE. From there, we list the major contributions of those studies and identify gaps between the proposed method and their method.

# Chapter 3 | Theory and Technical Approach

## *3.1. Introduction*

This chapter describes the theory and method used to build the framework. Section 3.2 describes the importance of system development in the lifecycle. Section 3.3 describes the approach to integrating multi-criteria impact analysis in the system development lifecycle. Section 3.4 describes integrating the multi-criteria impact analysis within the SysML methodology by exporting XMI files to Python scripts. Section 3.5 summarizes this chapter's contribution.

## *3.2. System Development Lifecycle*

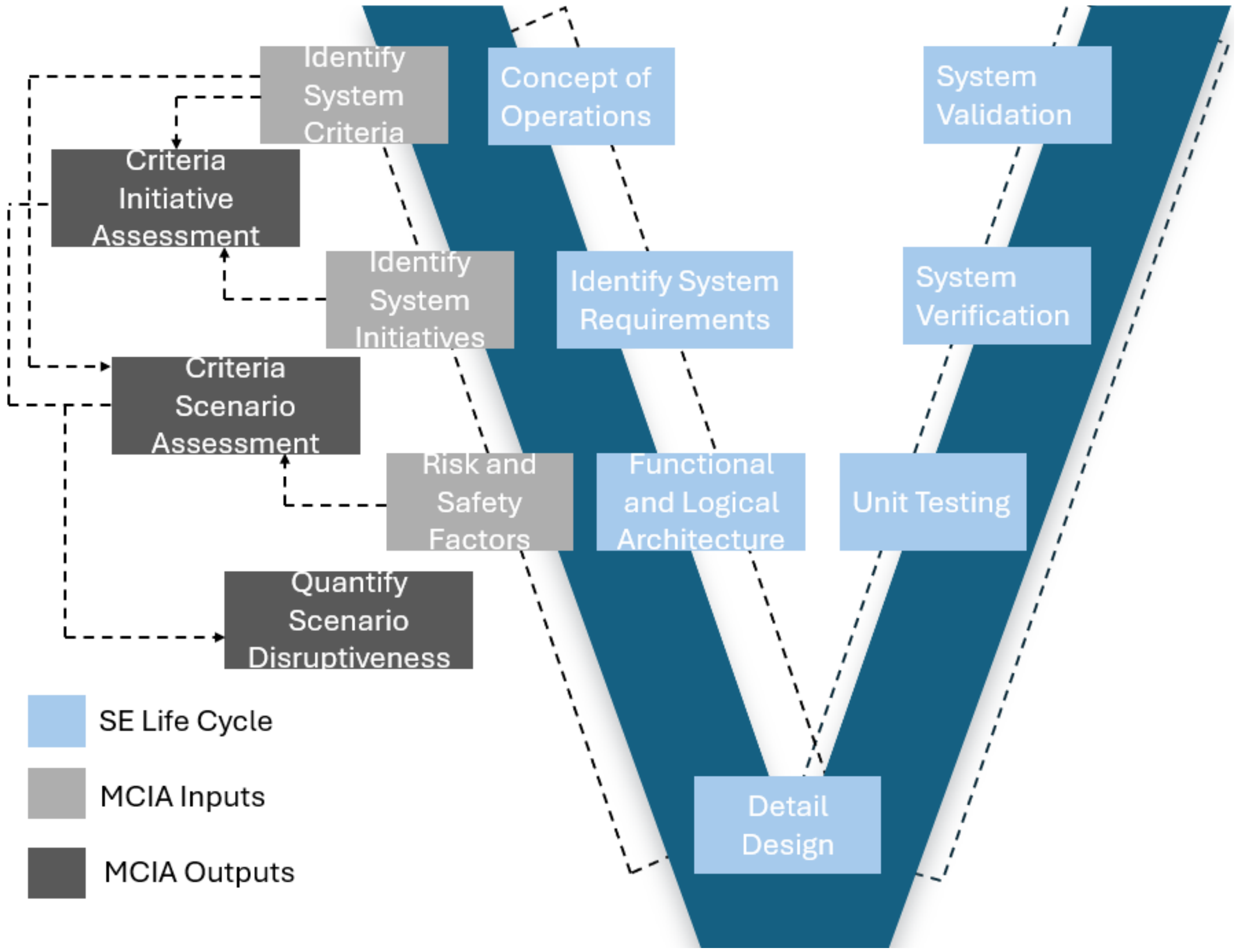



**FIGURE 4. Illustrates integrating the Model-Based System Engineering (MBSE) life cycle with Multicriteria Initiative Assessment (MCIA) inputs and outputs. The MBSE life cycle includes stages such as Concept of Operations, System Requirements, Functional and Logical Architecture, Detail Design, Unit Testing, System Verification, and System Validation. MCIA inputs and outputs, including identifying system criteria and initiatives and assessing scenarios and criteria, interact with various stages of the MBSE life cycle.**

Figure 4 illustrates the system development process using the V-model framework. The process starts at the top left with the concept of operations. Moving down to the left side of the 'V,' we outline the steps involved in system development. As the V ascends the right side of the 'V,' the focus shifts to system integration. This structure delineates the essential phases and sub-steps required for effective system development, ensuring that engineers follow a logical and comprehensive approach.

The concept of operations (CONOPS) is a document that describes a proposed system concept and how that concept operates in an intended environment. It is developed to identify system capabilities from the perspective of stakeholders and the system's operational scenarios. CONOPS is a time-ordered list of sequence steps or a graphical representation.

System requirements are vital to the system development life cycle and are defined after identifying the CONOPS. SEBoK defines system requirements as a statement that identifies system, product, or process characteristics or constraints, which is unambiguous, precise, unique, consistent, stand-alone, and verifiable and is deemed necessary for stakeholder acceptability (INCOSE 2010; ISO; IEEE). Identifying the system requirements is to produce a product that fits and goes beyond expectations, such as customer satisfaction, accurate budgeting, and schedule compliance. System requirements are captured using a requirements diagram.

High-level design is derived from combining the concepts of operations and system requirements. After implementation, it aims to provide all relevant stakeholders with a bird's-eye view of the solution architecture and design (Ltief, 2024).

### *3.3. Multi-Criteria Impact Analysis*

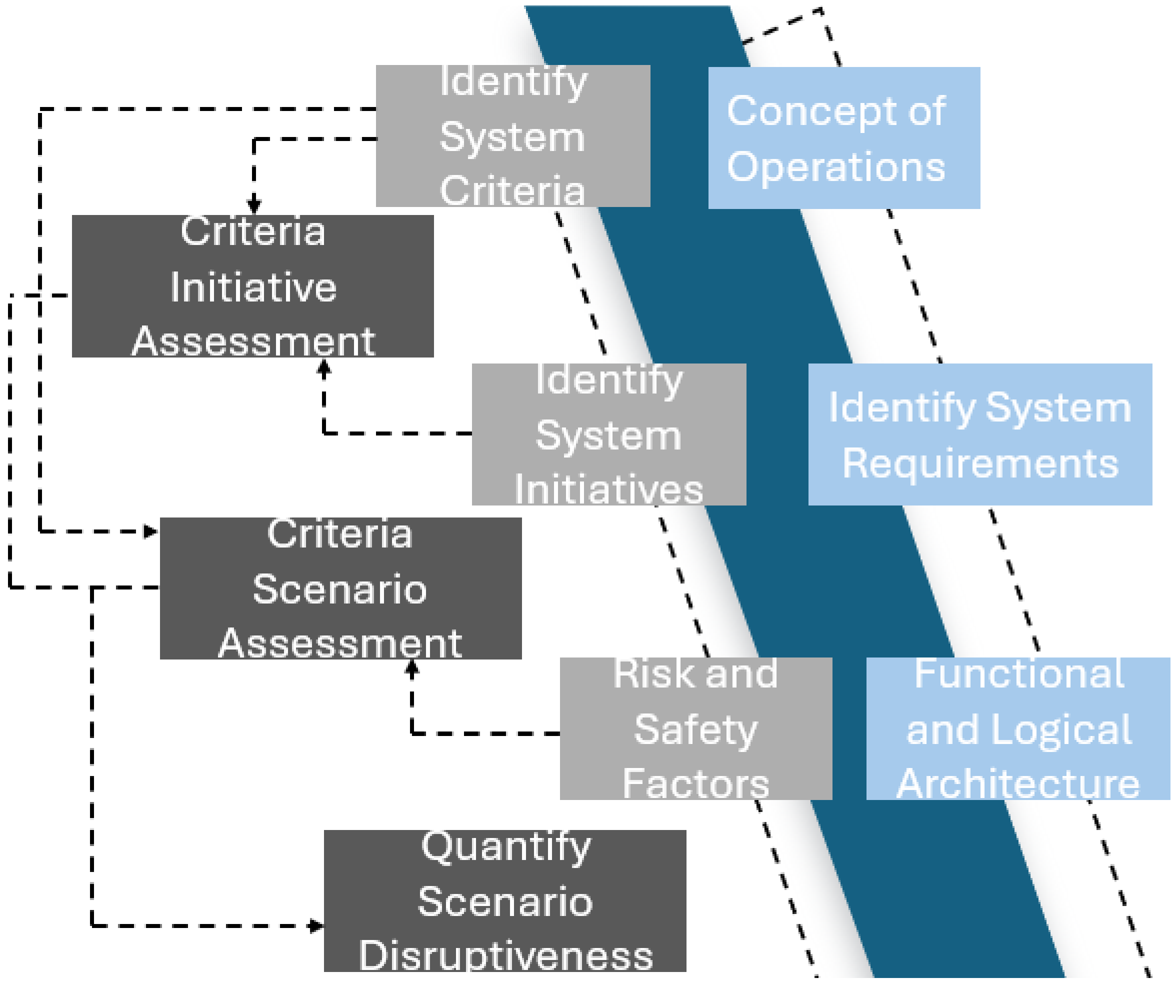



**FIGURE 5. The descending side of the vee model represents the early conceptual systems engineering life cycle. For this study, the model is coupled with the MCIA framework, which consists of integrating risk and safety factors into system development.**

This section describes how concepts from the STAMP analysis are integrated into the systems development lifecycle to integrate risk and safety factors into SysML.  Figure 5 a represents the descending of the V model linking with the multi-criteria impact analysis. Criteria and concept of operations

System criteria are performance objectives deviating from stakeholder elicitation and literature review. A framework is established to assess the potential influence of incorporating system models by defining the relationship between the system model and the criteria used for measurement. The set of system criteria is $C = \{c_1, c_2, \dots, c_m\}$. Representatives and system experts establish the baseline criteria to assess each criterion under regular conditions. Criterion can be scored by weight. The table describes how the weights were assigned as 0, 1, 2, and 4, corresponding to (-), *Low*, *Medium*, and *High*, respectively.

**TABLE 3. Criteria relevance importance weights.**

| Criteria Relevance | Weight |
|---|---|
| *High* | *4* |
| *Medium* | *2* |
| *Low* | *1* |
| - | *0* |

According to (Krishnan, 2020), a system engineering life cycle begins with concepts of operations which involve determining system capabilities from the viewpoints of its stakeholders and the operational scenarios of capabilities. The risk-safety register's initial step is to collect system criteria, which are overarching goals identified by stakeholders. Stakeholder-identified scenarios capture the most important stakeholder values.

The second step of this methodology is to capture the model. This requires the modeler to understand what a failure-free system would look like. This can be done using an activity diagram or a use case diagram. System models are representatives used to capitulate, analyze, and communicate information about a system or concept (Wynmore, 1993).

The set of initiatives is denoted as $X = \{x_1, x_2, \dots, x_n\}$. Initiatives consist of assets, projects, actions, technologies, or policies being considered for prioritization. This study extends the previous definition of initiatives by including using elements from SysML to represent actions originating from systems requirements and stakeholder needs.

According to (SEBoK, 2023), system requirements are utilized to identify a product or process operation, functional, or design characteristic or constraint, which is unambiguous, testable, measurable, and necessary for product or process acceptability. Requirements are captured in the SysML model using requirement diagrams. This step is combined with identifying initiatives; in this study, initiatives are a set of functions closely related to system requirements.

The third step of this methodology is to formulate emergent conditions. Traditionally, emergent conditions are denoted s $E = \{e_1, \ldots, e_k\}$ future events, policies, or conditions which may affect the value of initiatives within the system. The conditions are generally based on various sources, such as academic and industry stakeholders. The study extends the previous definition of emergent conditions by partitioning the set of emergent conditions into two categories. Therefore, the study utilizes the identification and management of risk and safety factors and categorizes them as emergent conditions. The innovation of this method is the ability for users to group positive controls, known as safety factors, as an emergent condition. Traditionally, adverse trends and events have always been categorized as disruptive orders. This study considers safety factors being grouped as an emergent condition to prove that they are just as disruptive as risk factors. This step is derived from the STAMP analysis. In STAMP, accidents are conceived as resulting not from component failures but from inadequate controls and constraints. Leveson describes STAMP as a method that emphasizes that safety concerns occur when control mechanisms cannot adequately enforce these essential constraints. This step includes the collection and formation of scenarios.

Scenarios denoted as $S = \{s_1, \ldots, s_j\}$ consist of one or more emergent conditions designed to depict the most significant challenges or risks that impact systems objectives on a broader scale. For all scenarios that exist, they are a subset of emergent conditions.

The third step of the SE life cycle is implementing a functional architecture. A functional architecture represents the functions that deliver on the system requirement. A SysML activity diagram captures the functions and their interactions with one another. Functions are captured in the SysML model using activity diagrams. The functional architecture is designed to reveal the order of functions within the system. The logical architecture defines the system's structural framework, which identifies the functions of various blocks or subsystems and describes the data flows and connections between them. When combined, block definition diagrams and internal block diagrams depict this architecture and show the structural relationships and functional interdependencies of the systems. This conceptualization helps to organize and visualize the overall functional flow of a system.

The next step is the criteria-initiative assessment. This step evaluates how effective each model initiative aligns with the success criteria for various elements within the system model, stakeholders from diverse backgrounds can conduct interviews and draw upon relevant literature to inform their analysis of the criteria-initiative (C-I) assessment. In this C-I assessment, stakeholders gauge the extent to which an initiative aligns with each criterion, using the following representations: a dash (-) for neutral, an unfilled circle (○) for somewhat agree, a half-filled circle (◐) for agree, and a filled circle (●) for strongly agree within the assessment matrix. The corresponding value is suggested to be $\{0, \frac{1}{3}, \frac{2}{3}, 1\}$.

**TABLE 4. Criteria-Initiative assessment weights.**

| Criteria-Initiative Assessment | Degree | Weight |
|---|---|---|
| ● | *strongly agree* | *1* |
| ◐ | *agree* | *0.667* |
| ○ | *somewhat agree* | *0.334* |
| - | *neutral* | *0* |

The qualitative results of the constraint matrix are converted into numerical weights following the rank-sum weighting method based on Equation 1:

$$W_j = \frac{m - rank_{j+1}}{\sum_{j=1}^{m} m - rank_{j+1}} \rightarrow \forall_j \in C \quad (1)$$

Let $w_j$ represent the weight assigned to the *j*-th criterion among a total of, *m* criteria, and $rank_j$ denote the ordinal ranking of this *j*-th criterion.

The following step is the criteria-scenario assessment. This evaluation presents how impactful a system criterion is on a scenario. The evaluation aims to answer the following: The importance of the criteria shifts depending on the baseline scenario presented. Responses are as Decreases, Decrease Somewhat, Neutral, Increases, and Increases Somewhat. Each response has an α associated with it in the $\alpha = \{\frac{1}{8}, \frac{1}{6}, 1, 6, 8\}$. The scaling constant aligns with the principles underlying the swing weighting approach. This method of swing weighting allows for modifications to account for various scenarios. The process of ascertaining weights for an additive value function through the swing weight technique is comprehensively detailed within the Multi-Criteria Impact Analysis (MCIA) field, and it is supported by numerous publications in this area.

**TABLE 5. Criteria-scenario important change**

| Criteria-Scenario Relevance | Weight |
|---|---|
| *Increases* | *8* |
| *Increases Somewhat* | *6* |
| - | *1* |
| *Decreases Somewhat* | *0.1667* |
| *Decreases* | *0.125* |

The swing weight method was utilized to establish the foundational weights ($W_j$) for the criteria, as well as to calculate the adjusted weights tailored to each specific scenario.

$$W_{jp} = \alpha * W_j \rightarrow \forall_j \in C, \forall_p \in S \quad (2)$$

Table 4 presents the allocation of weights to the various criteria pertinent to each scenario, with these alterations being captured within the W matrix.

Equations define $v_j(x_i)$ as the partial value function for the initiative $x_i$ concerning criterion $c_j$, established via the C-I assessment process. The matrix $V$ encapsulates the relative importance scores assigned to each initiative under various scenarios.

$$V_p(x_i) = \sum_{j=1}^{m} w_{jp} v_j(x_i) \rightarrow \forall_i \in X, \forall_p \in S, \forall_j \in C \quad (3)$$

For each scenario, initiative scores are ranked from 1 to $n$. Equation 4 outlines this ranking mechanism, where the symbol $>$ signifies that one initiative is of higher ordinal rank than another. Specifically, if the score of the initiative $x_i$ surpasses the score of $x_a$, then $x_i$ is awarded a higher ordinal position, such as being ranked $1^{st}$ compared to the $2^{nd}$ rank of $x_a$.

$$IF\ V_p(x_i) > V_p(x_a)\ THEN\ x_i > x_a \rightarrow \forall_{i,a} \in X, \forall_p \in S \quad (4)$$

To compute the disruptiveness score, one evaluates how much the priority rankings of initiatives shift under a specific scenario. Disruptiveness quantifies the extent of change in the priority order relative to a baseline scenario. This is calculated by summing up the squared differences in priority positions for each initiative when compared to their standings in the baseline scenario. Equation 5 details the formula for assessing the disruptiveness score for a given scenario $s_p$.

$$D_p = \sum_{i=1}^{n} \left(r_{i0} - r_{ip}\right)^2 \rightarrow \forall_i \in X, \forall_p \in S \quad (5)$$

$r_{ip}$ is the rank of initiative $x_i$ under scenario $s_p$ , and $r_{i0}$ is the rank of initiative $x_i$ under the baseline scenario. These scores are then normalized on a 0-100 scale (Almutari et al., 2018; Moghadasi et al., 2022).

## 3.4. Approach to Prioritizing System Order in SysML

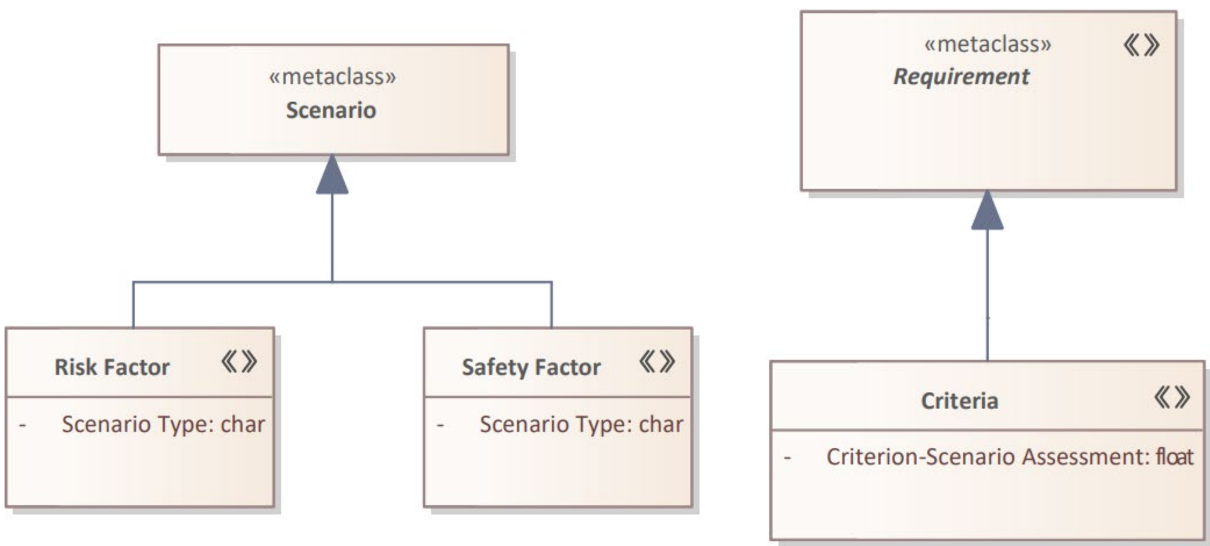



**FIGURE 6. The risk-safety profile for the system development stage process utilizes custom stereotypes to represent information related to multicriteria impact analysis. In this context, a scenario acts as a meta-class that aggregates risk and safety factor stereotypes in SysML. Additionally, the native SysML requirement meta-class is extended to include system criteria, enhancing its capability to capture essential system requirements.**

The framework integrates multi-criteria impact analysis by using SysML profiles to store the SysML model's risk factors and safety factors data. Consequently, no model transformation is required to create the model and generate the risk and safety artifacts. Figure 6 illustrates the risk and safety profile for the given framework. The framework follows the steps of employing the scenario-based multi-criteria decision model. For example, ‘Scenarios’ are derived from the action meta-class and extend the risk factors and safety factors stereotype, which contains attributes to capture risk. The risk factor and safety factors both fall under a disruptive scenario which influences the order of the functions. Meanwhile, the safety factor in the system's profile is assigned an effectiveness score that measures the influence a risk or safety factor has on a *Criteria stereotype*. This analysis is followed by the categorization of risk and safety factors and measure by the impacts on said initiative.

On the other hand, the *Criteria*” stereotype is utilized to store the performance metrics used to evaluate the system’s objectives. The system associates a weight value for the criteria which was described earlier in the previous section. The study stores the C-I assessments through the activities within the functional architecture. However, the scores associated with criteria-scenario assessment are stored within the criteria stereotype. The purpose of storing the scores within the profile is to communicate amongst stakeholders the values associated with the components within the system model.

The study's methodology employs activity diagrams to clarify the interactions within the system model, providing a visual representation of information flow. These interactions are identified as initiatives that are integral to the functional architecture, which outlines the system's operational framework. To effectively capture safety and risk factors within the model we extend the safety and risk artefacts.

The Python code is designed to parse criterion information while extracting the weight of each criterion. Risk and safety analysts are tasked to enter scores corresponding to the C-I and C-S assessments.

```
def parse_activity_diagrams(xmi_file):
    with open(xmi_file, 'r', encoding='utf-8') as file:
        xmi_content = file.read()

    root = etree.fromstring(xmi_content.encode('utf-8'))
    ns = {
        'xmi': 'http://schema.omg.org/spec/XMI/2.1',
        'uml': 'http://schema.omg.org/spec/UML/2.1'
    }

    activities = root.xpath('//packagedElement[@xmi:type="uml:Activity"]', names
    print(len(activities), "activities found with adjusted XPath")

    activities_data = []
    seen_names = set()  # Set to store names of activities already processed

    for activity in activities:
        activity_id = activity.get('{http://www.omg.org/spec/XMI/2.1}id')
        activity_name = activity.get('name')

        # Check if the activity name is already seen
        if activity_name not in seen_names:
            # If not, add the activity data and mark the name as seen
            activities_data.append({'Activity ID': activity_id, 'Activity Name':
            seen_names.add(activity_name)

    print(activities_data)
    return activities_data
```

**FIGURE 7. The code defines a function to parse activity diagrams from an XMI file. It reads the file, extracts activities while preventing duplicates, and collects their names and IDs. The result is a list of unique activities, which is then printed and returned.**

Figure 7 describes a Python script designed to parse activity diagrams from an XMI file, which is a standard file format for exchanging metadata information via XML. Specifically, this script appears to target activity diagrams related to risk and safety analysis.

```python
def parse_criterion_weight(xmi_file):
    with open(xmi_file, 'r', encoding='utf-8') as file:
        xmi_content = file.read()

    root = etree.fromstring(xmi_content.encode('utf-8'))
    criteria_data = []

    ns = {
        'xmi': 'http://schema.omg.org/spec/XMI/2.1',
        'uml': 'http://schema.omg.org/spec/UML/2.1'
    }

    # XPath targeting element with a classifier attribute
    # Corrected variable name to 'criteria_elements' to match the loop
    criteria_elements = root.xpath(
        './/element[@classifier="EAID_47051B99_8419_4249_A35C_0F44EFEF11BB"]',
                                          namespaces=ns)

    for elem in criteria_elements:  # Correct variable name used here
        criterion_name = elem.get('name')
        criterion_id = ''
        weight = ''

        # Find attributes within each criterion element
        for attr in elem.xpath('.//attribute', namespaces=ns):
            if attr.get('name') == 'Criterion ID':
                criterion_id = attr.xpath('.//initial/@body', namespaces=ns)[0]
            elif attr.get('name') == 'Weight':
                weight = attr.xpath('.//initial/@body', namespaces=ns)[0]

        criteria_data.append({
            'Criterion Name': criterion_name,
            'Criterion ID': criterion_id,
            'Weight': weight
        })

    return criteria_data
```

**FIGURE 8. Extracting criteria and their weights from an XMI file to create a structured list of data with names, ID, and associated weights using XML parsing and XPath queries in Python.**

Figure 8 describes a Python function designed to parse criterion information while extracting the weight of each criterion. Risk and safety analysts are tasked to enter scores corresponding to the C-I and C-S assessment within the functional diagrams and the

```
def parse_criteria_initiative_assessment(xmi_file):
    try:
        with open(xmi_file, 'r', encoding='utf-8') as file:
            xmi_content = file.read()
    except Exception as e:
        print(f"Error reading criteria initiative assessment: {e}")
        return []

    try:
        root = etree.fromstring(xmi_content.encode('utf-8'))
    except etree.XMLSyntaxError as e:
        print(f"XML Syntax Error: {e}")
        return []

    ns = {'xmi': 'http://schema.omg.org/spec/XMI/2.1'}
    criteria_initiative_assessment_data = []

    # Assuming 'element' is the correct tag and not 'packagedElement' based on your XML structure.
    elements = root.xpath('//element[@xmi:type="uml:Activity"]', namespaces=ns)

    for element in elements:
        activity_name = element.get('{http://schema.omg.org/spec/XMI/2.1}name')
        print(f"\nProcessing activity: {activity_name}")

        attributes = element.xpath('.//attribute', namespaces=ns)

        if not attributes:
            print(f"No attributes found for activity: '{activity_name}'")
            continue

        for attribute in attributes:
            attr_name = attribute.get('{http://schema.omg.org/spec/XMI/2.1}name')
            initial_body = attribute.xpath('.//initial/@body', namespaces=ns)
            value = initial_body[0] if initial_body else 'N/A'

            print(f"Found attribute - Name: {attr_name}, Value: {value}")

            criteria_initiative_assessment_data.append({
                'Activity Name': activity_name,
                'Attribute Name': attr_name,
                'Value': value
            })

    if not criteria_initiative_assessment_data:
        print("No attributes found in any activities.")

    return criteria_initiative_assessment_data
```

**FIGURE 9. The 'parse_criteria_initiative_assessment' Function — Efficiently extracts activity criteria from XMI files, robustly manages XML syntax errors, and compiles attributes. It yields a neatly organized dataset comprising activity names, attribute names, and corresponding values.**

Figure 9 describes the Python script representing the Python function for parsing criteria initiative assessment. It describes the process of extracting criteria names within initiatives. The scores corresponding with C_I assessments are then transferred for all initiatives and stored within a matrix.

```
def emergent_conditions(xmi_file):
    logging.basicConfig(level=logging.INFO)
    logging.info(f"Starting emergent_conditions function with file: {xmi_file}")

    try:
        with open(xmi_file, 'r', encoding='utf-8') as file:
            xmi_content = file.read()
    except Exception as e:
        logging.error(f"Error accessing file {xmi_file}: {e}")
        return []

    try:
        root = etree.fromstring(xmi_content.encode('utf-8'))
    except Exception as e:
        logging.error(f"Error parsing XML: {e}")
        return []

    ns = {
        'xmi': 'http://schema.omg.org/spec/XMI/2.1',
        'uml': 'http://schema.omg.org/spec/UML/2.1',
    }

    # Corrected XPath to match 'packagedElement' tags with the specified type attribute
    specific_elements_with_type = root.xpath('//packagedElement[@xmi:type="uml:InstanceSpecificatior
    logging.info(f"Total elements found with adjusted XPath: {len(specific_elements_with_type)}")

    element_names = [elem.get('name') for elem in specific_elements_with_type if elem.get('name')]
    for name in element_names:
        logging.info(f"Found Object: {name}")

    if not element_names:
        logging.info("No matching elements found with adjusted XPath. Consider reviewing the XPath e

    return element_names
```

**FIGURE 10. The 'emergent conditions' Function — Streamlines the extraction of element names from an XMI file, integrates error handling for file access and XML parsing, and leverages logging for process insights.**

Figure 10 describes a Python script that extracts the name of the emergent condition whether it is listed as a risk factor or safety factor. The risk and safety factors are transferred to a spreadsheet. Users operating the spreadsheet shall be able to organize risk and safety factors for the scenarios.

## *3.5 Summary*

The chapter describes the system design life cycle, an approach used for the development of complex systems. The chapter introduces a mathematical decision framework approach to integrating risk and safety factors within the system development life cycle. This framework extracts elements from SysML to determine which elements are most vulnerable to disruptions stemming from risk and safety factors. Chapters 4 and 5 demonstrate the application of the method for diverse case studies.

# Chapter 4 | Case Study Smart Parking Lot System

## *4.1. Introduction*

This chapter describes applying a framework to understand how system order is disrupted in a smart parking lot system within a smart city. The section below describes motivation, for example.

Rapid industrialization and population growth in urban centers have significantly increased the number of vehicles, leading to numerous mobility challenges (Alsafery et al., 2018). These challenges include increased traffic congestion, higher emissions, and inefficient use of urban space. Among the promising solutions to these issues are smart parking systems, particularly those based on Internet of Things (IoT) technologies. These systems have gained prominence due to their ability to effectively address urban mobility issues by optimizing parking space utilization. Studies support that smart parking systems can significantly reduce their time and resources cruising for available parking spots (Zulfiqar et al., 2023; Papp Mobility, 2023; Ouhammou et al., 2023; Mifra Electronics, 2024; Paradox Engineering, 2024), highlighting the critical need for efficient parking management solutions.

Despite technological advancements, developers often overlook comprehensive risk-safety integration when creating smart parking systems. This gap can lead to system vulnerabilities and inefficiencies, jeopardizing reliability and safety. To enhance the resilience and performance of smart parking systems, developers must systematically incorporate risk-safety factors into the system development life cycle. Failure to implement risk and safety measures often leads to costly changes that are avoidable before the system is integrated.

This chapter addresses this gap by utilizing a Risk-Safety Profile to identify and mitigate risks within the system development life cycle of a Smart Parking Lot System. The section focuses on integrating risk-safety factors into each phase of system development to ensure that potential hazards are identified and managed effectively. Essentially, SysML is utilized to visually display the information flow within the system.

The approach begins by engaging stakeholders and reviewing relevant literature to establish system criteria and the concept of operations. This process is followed by defining system requirements and initiatives. The risk and safety factors will be integrated into a custom SysML profile, encompassing a high-level design. Additionally, criteria-initiative and criteria-scenario (C-S) assessments will be conducted to rank initiatives and identify disruptive scenarios.

## *4.2. Application of Multi-Criteria Impact Analysis on Smart Parking Lot*

### *4.2.1. Concept of Operations and System Criteria*

This section describes the approach to integrating risk and safety factors within SysML diagrams and transfers the safety and risk metrics to conduct an MCIA from the SysML model. The primary focus of the study is to evaluate the application of the risk and safety factors framework. The Smart Parking Lot Systems identifies the need to achieve objectives that are aligned with the concept operations.

**TABLE 6. The concept of operation for a generalized system of the interactions of a smart parking lot within a smart city was adapted from (INCOSE, 2023).**

| Stakeholders | Capabilities |
|---|---|
| Driver | **Parking Vehicle** |
| | **Retrieve Vehicle** |
| | **Reserve Parking Slot** |
| | **Parking Available Information** |
| Municipal Corporation | **Monitoring and Management** |
| | **Data collection and analysis** |
| | **Public information** |
| Law Enforcement | **Vehicle Tracking** |
| | **Security and Surveillance** |
| Smart City Control Center | **Integration and Coordination** |
| | **Centralized Management** |
| | **Data Aggregation** |

| | |
|---|---|
| Third-Party App Developers | **API Integration**<br>**Interoperability** |
| Payment System Providers | **Flexible Payment Options**<br>**Secure Transaction** |
| Internet Service Providers | **Connectivity and Reliability** |

Within the context of a smart parking lot system, stakeholders and elements are critical to the system. The stakeholders include the driver, smart city control center, municipal corporation, and law enforcement. The elements include a Parking app, smart city control center, internet, and payment system. The study will examine operations between elements and stakeholders using activity diagrams.

The framework's first step is identifying criteria based on the concept of operations. The criteria of the case study are mentioned in the table:

Table 6 describes the concept of operations by listing stakeholders in the left column and listing specific capabilities in the right column. The stakeholders include the driver, smart city control center, municipal corporation, and law enforcement. The elements include a Parking app, smart city control center, internet, and payment system. For example, within their capabilities, law enforcement are responsible for acting as security and surveying the smart parking lot, and their role may be intertwined with tracking down suspects that have stolen vehicles from

Table 7 describes seven success criteria identified for a smart city's smart parking lot system, adapted from several sources (Joshi, 2021; Ajchariyavanich et al., 2019; Rehena et al., 2018). The seven success criteria are aligned. *C.01 – Reduction of Traffic Congestion* refers to a system that reduces the time drivers spend searching for parking and can significantly decrease the volume-to-capacity ratio. *C.02 – User Experience* refers to real-time information about parking and reservations, saving time and reducing frustration (Li et al., 2021). *C.03 – Efficient Use of Parking Space* refers to how the system ensures that all parking spots are used deficient. It maximizes the use of parking resources (Aydin et al., 2017). *C.04 - Cost and Resource Efficiency* refers to the minimization of the need for parking staff; smart parking systems can reduce operational costs and improve resource allocation (Mangiaracina et al., 2017). *C.05 – Environmentally* reducing dwell time is associated with seeking a parking space and lowering fuel consumption and emission (Ramaswamy, 2016). *C.06 – Integration with Smart City Infrastructure* refers to how the smart parking lot system utilizes IoT technologies and cloud systems to integrate smart parking with smart city initiatives (Dobrzański et al., 2023). *C.07 – Flexibility and Scalability* refers to the system's design accommodating varying conditions (Iacobescu et al., 2021).

**TABLE 7. Success criteria are used to evaluate the initiatives for the smart parking lot systems. Success criteria are adapted from a list of requirements and stakeholder elicitations.**

| Index | Criterion |
|---|---|
| *c.01* | Reduction of Traffic Congestion |
| *c.02* | User Experience |
| *c.03* | Efficient Use of Parking Space |
| *c.04* | Cost and Resource Efficiency |
| *c.05* | Environmental |
| *c.06* | Integration with Smart City Infrastructure |
| *c.07* | Flexibility & Scalability |

### *4.2.2. System Initiatives and System Requirements*

Table 8 describes twenty-one unique requirements based on requirement data collected from INCOSE (2023). For example, requirement ID 7 requires that the central computing system be able to operate at environmental temperatures up to 55 degrees Celsius. The requirements listed help establish functional and logical architecture.

**TABLE 8. Requirement table listing all requirements adapted from the (INCOSE, 2023)**

| ID | Description |
|---|---|
| *4* | Parking space shall be classified by type: two-wheeler, compact four-wheeler, or SUV type. |
| *7* | The Central Computing System shall be able to operate at environmental temperatures up to 55 degrees Celsius. |
| *8* | Database size shall be sufficient to store data for the previous 4 days. |
| *9* | Data storage shall adhere to security standards prescribed by Data Security. |
| *10* | Portable devices shall be designed for handheld operation. |
| *10.1* | The portable device shall weigh less than 250g. |
| *10.2* | The display should be readable under ambient lightning. |
| *12* | A portable device shall be able to read reservation QR codes from printed tickets or apps. |
| *14* | The REST API interface shall support the latest Transport Layer Security (TLS) standards. |
| *15* | The PHS shall support cash transactions. |
| *16* | The PHS shall support transactions through credit cards, net banking, and popular payments. |
| *18* | The PHS shall employ encryption for all data communication, both within the Parking lot's internal network as well as with external networks. |
| *19* | The intranet interface must employ SSL and WPA2 (or higher) security standards for communications. |
| *20* | The PHS shall ensure that charges do not exceed the prevailing maximum allowable rates published by the Smart City. |
| *21* | The Payment Systems shall employ daily validation of prevailing maximum allowable rates published by the Smart City. |
| *22* | Brightness should adjust to ambient lightning. |
| *23* | The Systems shall provide all API functions mandated by the Smart Parking standards. |
| *24* | The systems shall provide reservation confirmation in the form of a QR code conforming to the Smart City parking standards. |
| *25* | The System shall provide an entry ticket conforming to Smart City standards. |
| *26* | The system shall notify user of the expiry of their reservation at least minutes in advance. |
| *27* | The system shall follow zonal restrictions on the maximum percentage of reservable spaces and the maximum reservations period as per Smart City. |

Table 9-11 describes twenty-one, twenty-seven, and seventeen initiatives collected for the functions of entering the smart parking lot, reserving a parking lot, and retrieving a vehicle, respectively.

**TABLE 9. A list of initiatives is represented as functions necessary for an activity diagram for a vehicle to enter the smart parking lot.**

| Index | Initiatives |
|---|---|
| *x.01* | Drive to lot entrance |
| *x.02* | Show reservation confirmation |
| *x.03* | Request on the Spot Entry |
| *x.04* | Enter lot to park |
| *x.05* | Leave Parking Lot |
| *x.06* | Perform security check on vehicle |
| *x.07* | Scan reservation confirmation |
| *x.08* | Convey refused reservation |
| *x.09* | Allow entry and provide slot/level info. |
| *x.10* | Record vehicle details |
| *x.11* | Convey Space Unavailability |
| *x.12* | Record Entry |
| *x.13* | Form Submit |
| *x.14* | Display Slot Unavailability |
| *x.15* | Display Slot Assignment |
| *x.16* | Submit details |
| *x.17* | Display Refusal |
| *x.18* | Read Reservation Confirmation |
| *x.19* | Slot assignment |
| *x.20* | Check reservation validity |
| *x.21* | Record Entry |

Table 8 describes the initiatives related to the functions for entering a smart parking lot. For example, x.01 refers to Driving to the lot entrance, and the very last initiative, x.21, refers to recording entry, which is an integral part of having a smart parking lot system.

**TABLE 10. List of functions to capture the necessary activities for reserving a parking slot.**

| Index | Initiatives |
|---|---|
| *x.01* | Use parking application |
| *x.02* | Request reservation |
| *x.03* | Request parking with time and lot |

| | |
|---|---|
| *x.04* | Provide payment details |
| *x.05* | Check reservation availability & rates |
| *x.06* | Gather responses & display options |
| *x.07* | Request reservation |
| *x.08* | Generate payment gateway page |
| *x.09* | Send payment confirmation to parking lot |
| *x.10* | Display & save confirmation |
| *x.11* | Display reservation refusal |
| *x.12* | Confirm payment |
| *x.13* | Receive reservation availability & rate request |
| *x.14* | Receive reservation request |
| *x.15* | Calculate reservation availability & rate |
| *x.16* | Hold reservation slot |
| *x.17* | Provide reservation confirmation |
| *x.18* | Refuse Reservation |
| *x.19* | Log Payment confirmation & transaction details |
| *x.20* | Initiate Payment |

Table 10 does the same by referencing activities associated with reserving a parking slot within a smart parking lot system. Initiatives x.01—Use parking application and x.04—Check reservation availability rate are all unique to the parking spot reservation scenario.

**TABLE 11. List of functions that capture the necessary activities "retrieve vehicle" activity diagram from the smart parking lot system.**

| Index | Initiatives |
|---|---|
| *x.01* | Walk up to parked vehicle |
| *x.02* | Retrieve vehicle to exit |
| *x.03* | Show entry ticket |
| *x.04* | Inform lost ticket |
| *x.05* | Scan entry ticket |
| *x.06* | Verify ID and record car details |
| *x.07* | Collect Payment |
| *x.08* | Allow exit |
| *x.09* | Record exit |
| *x.10* | Record vehicle details |
| *x.11* | Convey Space Unavailability |
| *x.12* | Record entry |
| *x.13* | Read entry record from ticket |
| *x.14* | Submit information |
| *x.15* | Form submits |
| *x.16* | Calculate pending fees and penalty |
| *x.17* | Exit lot |

Table 11 refers to the last scenario of retrieving vehicles from the lot within the smart parking system. Initiatives such as *x.01*—Walk up to parked vehicle and x.07—Collect Payment are unique to the functional diagram.

### *4.2.3. Functional and Logical Architecture*

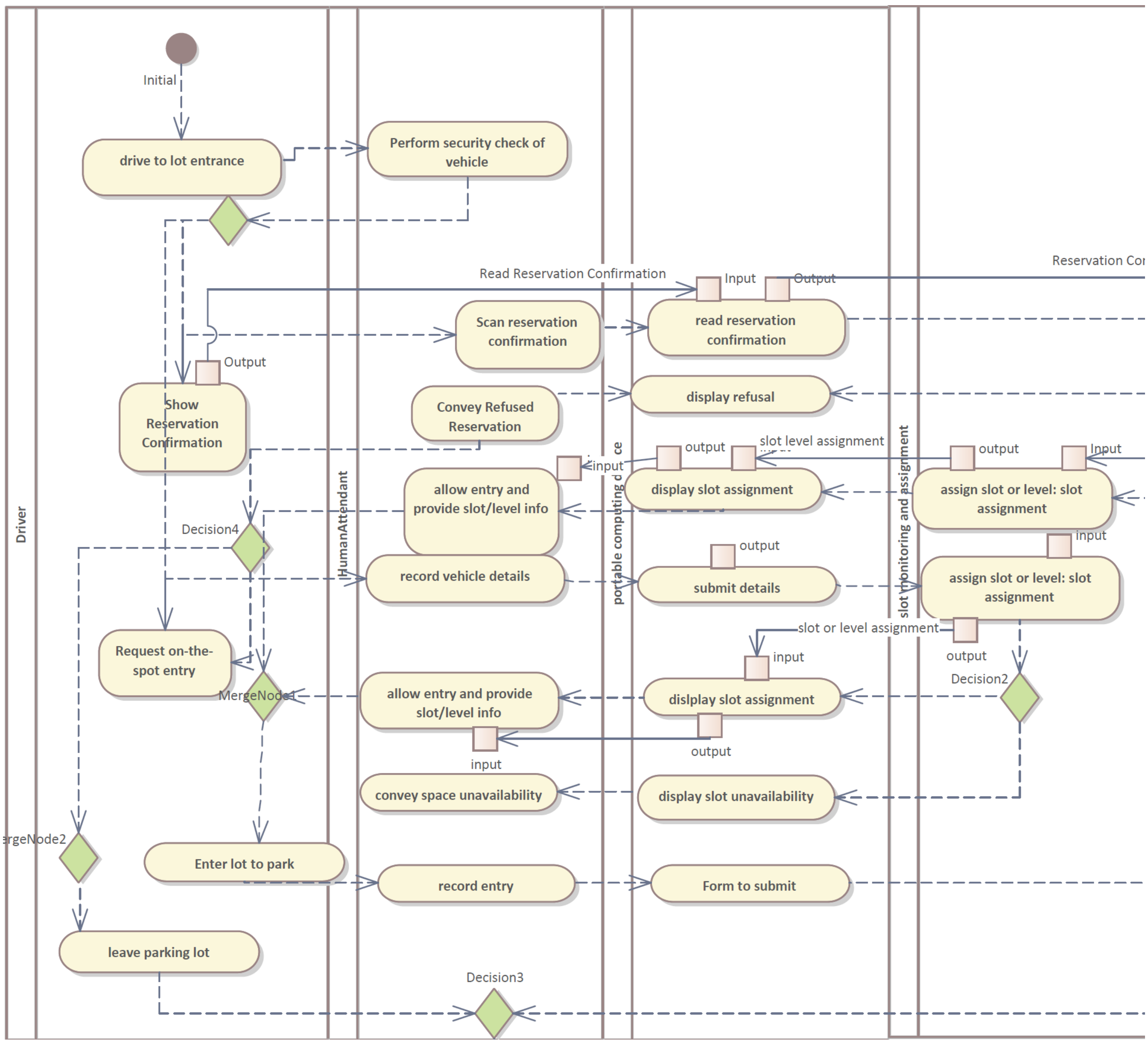



**FIGURE 11. The SysML Activity Diagram represents the functional architecture related to entering a smart parking lot for a smart city (Joshi et al., 2021).**

Figure 11 is a SysML activity diagram describing the workflow of retrieving a parking spot within a smart parking lot system. When the driver gets to the lot entrance, the procedure starts with a security check. The human attendant scans and confirms the driver's reservation if they have one, then either grants entry and provides information about the driver's slot or signals a refusal if the reservation is invalid. An entry request made on the spot for drivers without a reservation is considered. Availability is determined by slot assignment and monitoring; the system either assigns a slot or indicates it is unavailable. Lastly, vehicles ensure effective and well-organized parking management by entering the lot to park or leaving if a spot is unavailable.

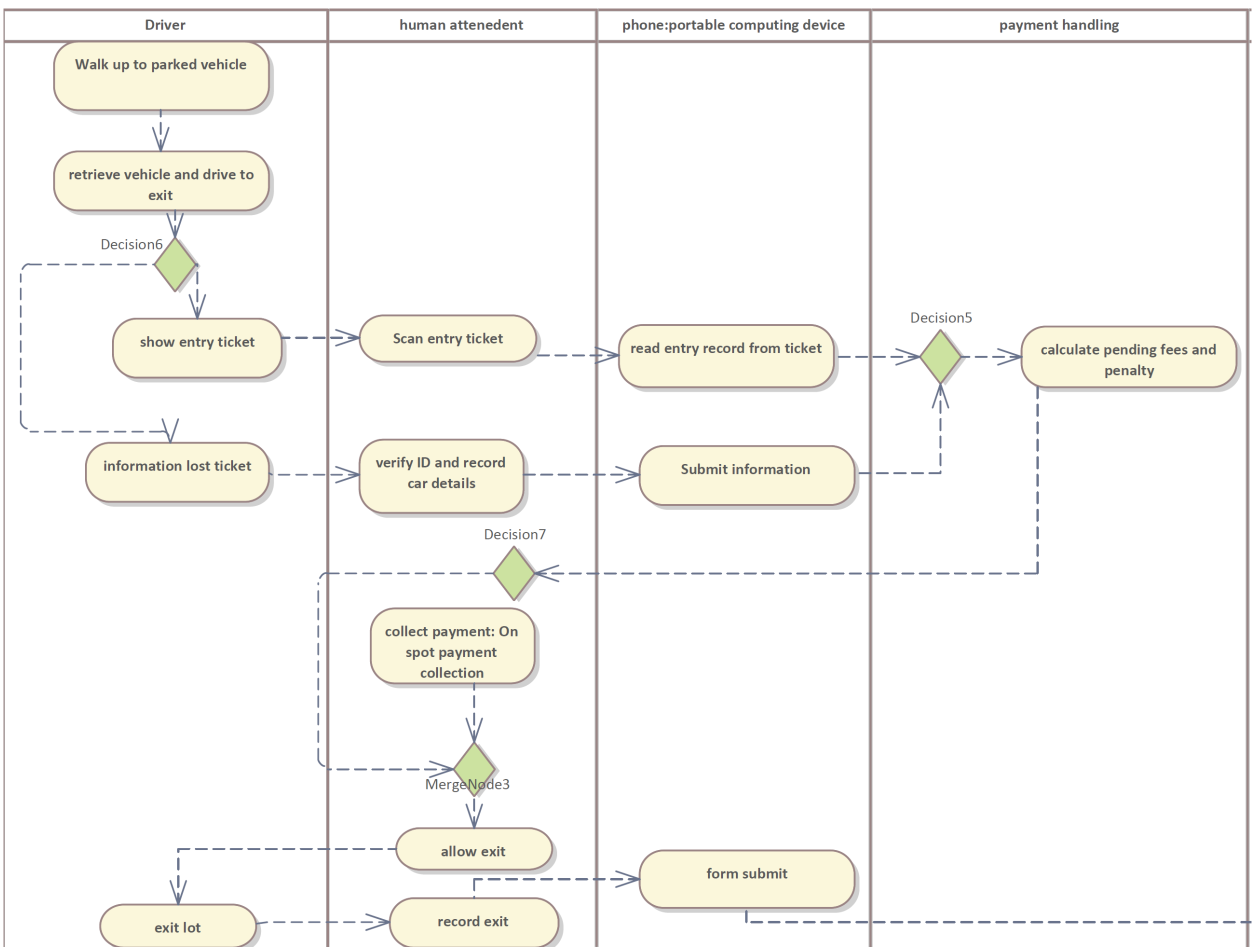



**FIGURE 12. SysML Activity Diagram represents the functional architecture related to a driver retrieving their vehicle and exiting the smart parking lot for a smart city. This activity partition describes the behavior that envisions the driver, human attendant, and portable computing device retrieving the vehicle adapted. Green diamonds represent the merge and decision nodes (Joshi et al., 2021).**

Figure 12 describes a SysML activity diagram for a driver retrieving their vehicle. After returning their car, the driver proceeds to the exit, where they must show their entry ticket or report a lost one. The human attendant takes down vehicle information, scans the entry ticket, and confirms the driver's ID. The information is submitted, and the entry record is read from the ticket using a portable computing device. One must determine whether fees are owed to handle payments and then compute any outstanding fines and penalties. The payment is then immediately collected by the human attendant. The driver leaves the lot after payment has been made or confirmed, and their exit is authorized and noted. This procedure, which includes payment and verification stages, guarantees the timely and organized processing of parking lot exits.

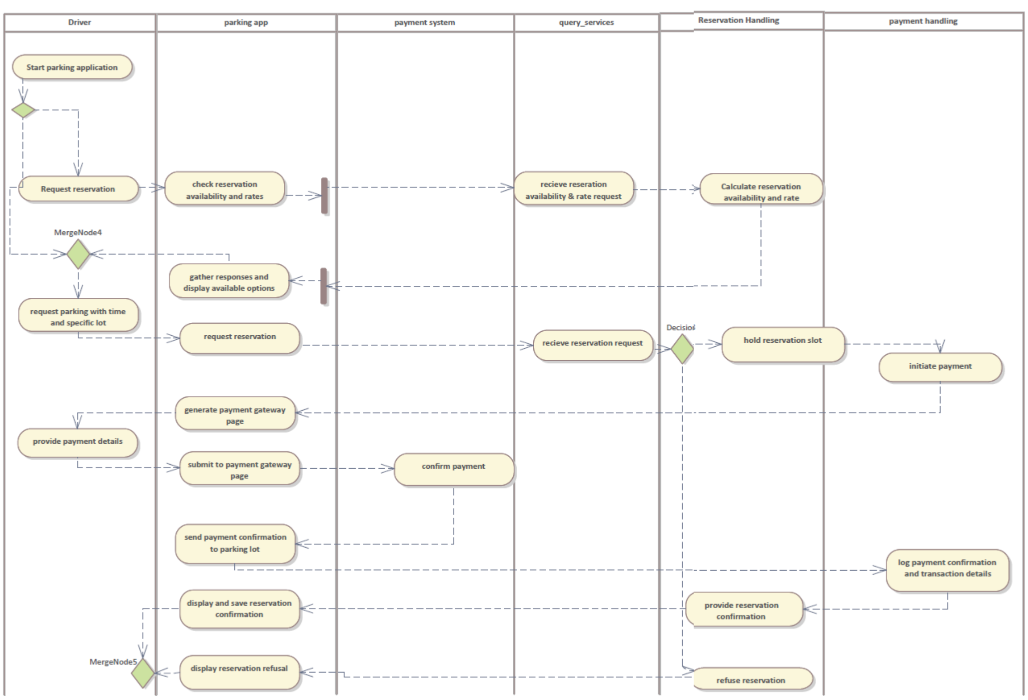



**FIGURE 13. The SysML Activity Diagram represents the functional architecture of utilizing the parking application for a smart parking lot. Green diamonds represent decision nodes adapted from (Joshi, 2021).**

Figure 13 is an envisaged functional architecture representing the scenario of reserving a parking space for the smart parking lot system. This sequence diagram captures the end-to-end process of making a parking reservation, from the driver's initial request to the confirmation of the payment and final reservation status. It outlines the interaction between different components in the system, ensuring a clear understanding of how each part of the system contributes to the overall process.

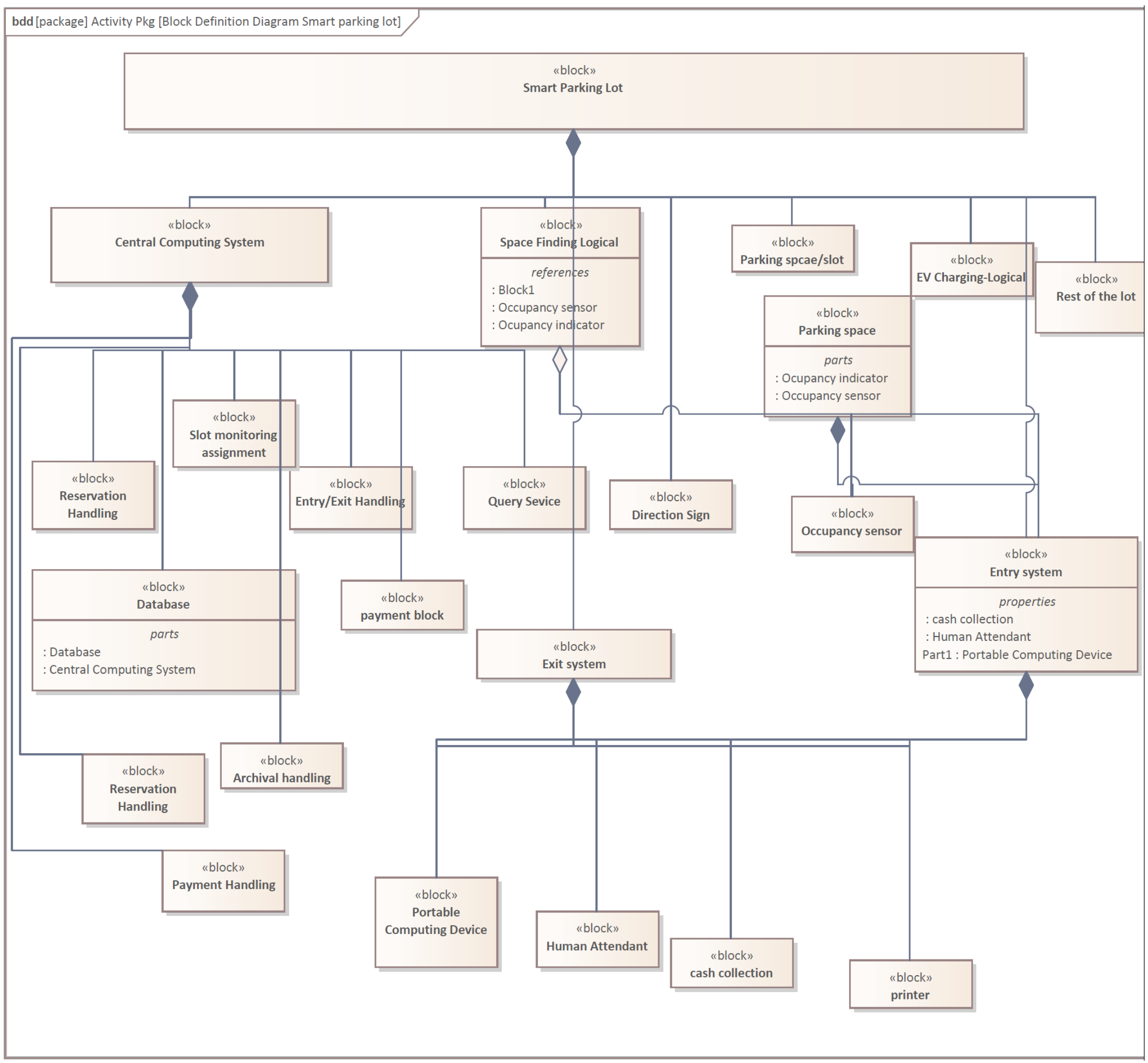



**FIGURE 14. SysML block definition diagram that illustrates the structural hierarchy of a Smart Parking Lot System for a smart city. It highlights various logical blocks within the system and the specific functions assigned to each block adapted from (Joshi et al., 2021).**

Figure 14. The main parts of the Smart Parking Lot system and how they work together are shown in the Block Definition Diagram. With the help of a database, the system consists of a Central Computing System that manages payments, entry/exit procedures, slot monitoring, and reservation handling. It integrates Space Finding Logic with occupancy sensors and indicators to manage parking spaces, including EV charging capabilities. Human attendants and mobile computers operate entry and exit systems, making information processing and money collection easier. To guarantee effective and well-organized parking operations, other components include printers, archival handling, direction signs, and a query service.

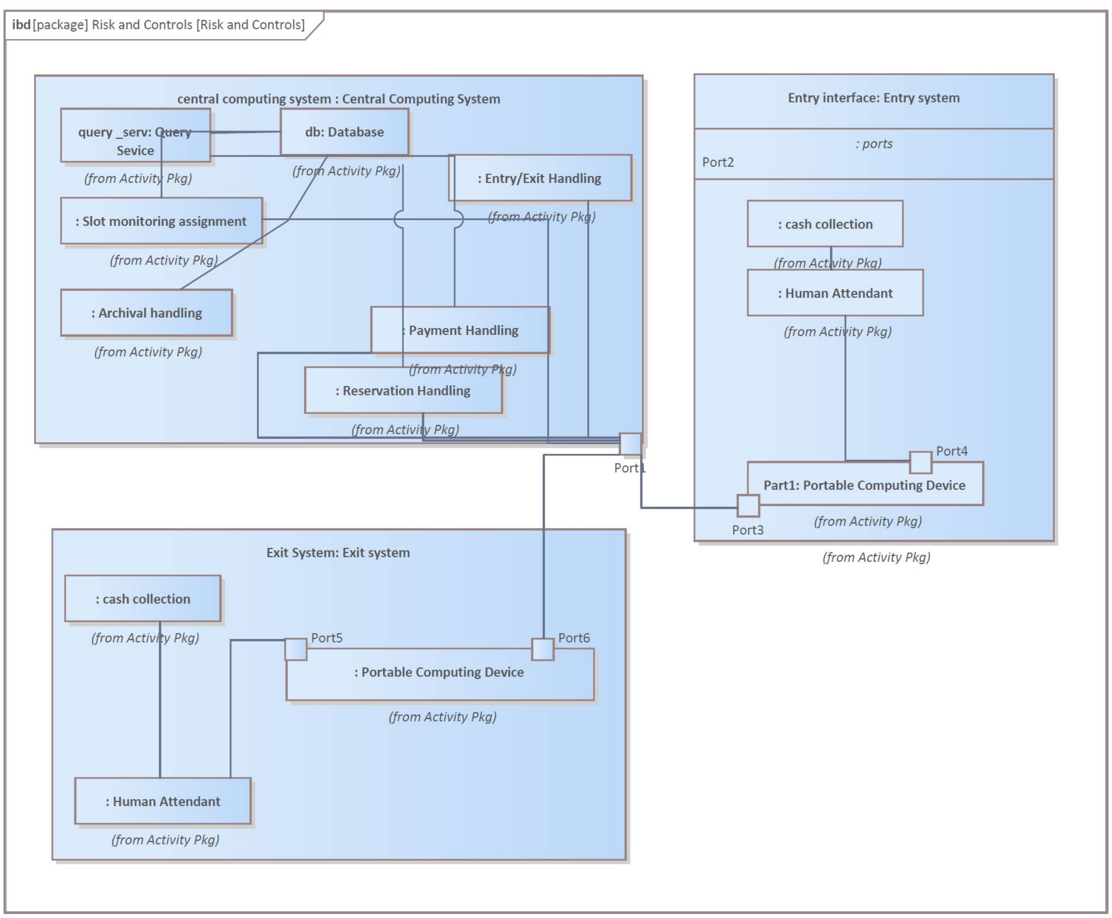



**FIGURE 15. SysML Internal Block Diagram illustrating the connections and interfaces between internal subsystems of the Smart City Smart Parking Lot System adapted from (Joshi et al., 2021).**

The Smart Parking Lot system's Internal Block Diagram (IBD) shows the internal organization and relationships between the parties in charge of risk and controls. With the aid of a central database, the Central Computing System oversees key operations like entry/exit handling, reservation handling, payment processing, slot monitoring, archival handling, and query services. The Entry Interface system integrates human attendants and cash collection components with portable computers to make entry operations easier. Comparably, the Exit System uses mobile computing devices to control vehicle exits, human attendants, and cash collection. The diagram illustrates how these subsystems and their constituent parts communicate via various ports to guarantee effective operation and control within the smart parking lot.

### *4.2.4. Applying Custom Stereotype to Functional Architecture*

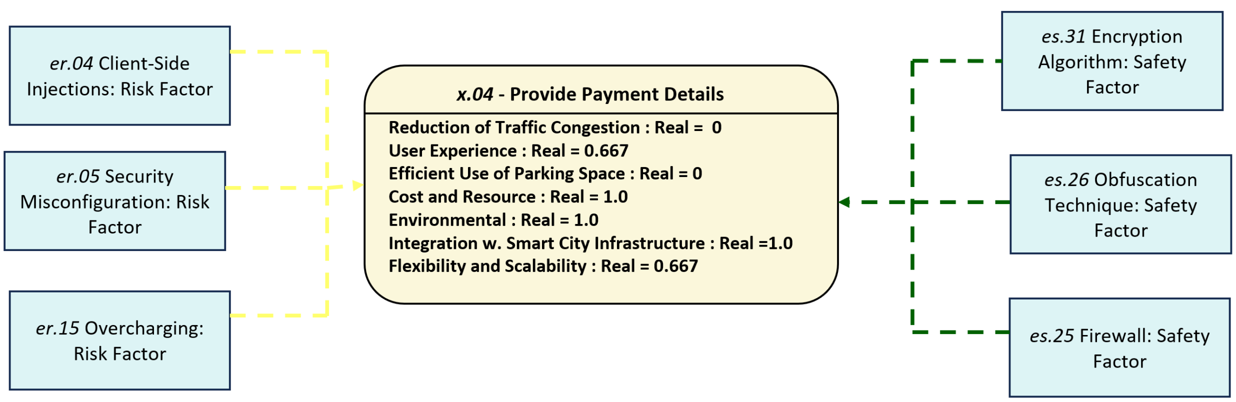



**Figure 16. Applying risk factors and safety factors for the function "Provide Payment Details" along with the *Criteria*-Initiative Assessment.**

Figure 16 shows how the risk-safety profile is applied to an activity within the functional architecture. The criteria are listed, followed by the datatype and the criteria initiative score, which indicates how well the initiative addresses the criteria. For example, activity x.04—Provide Payment Details holds values of the criteria-initiative assessment within the attributes, which define the properties or internal data elements of an element of a function.

Table 12 describes how all the criteria related to developing a smart parking lot system are of medium relevance to the other criteria.

**TABLE 12. Baseline relevance for the Smart Parking Lot System.**

| The Criterion c.xx has | s.00 – Baseline | Relevance among the other criteria |
|---|---|---|
| *c.01 - Reduction of Traffic Congestion has* | *medium* | Relevance |
| *c.02 – User Experience* has | *medium* | Relevance |
| *c.03 – Efficient Use of Parking Space* has | *medium* | Relevance |
| *c.04 – Cost and Resource Efficiency* has | *medium* | Relevance |
| *c.05 – Environmental* has | *medium* | Relevance |
| *c.06 – Integration with Smart City Infrastructure* has | *medium* | Relevance |
| *c.07 - Flexibility & Scalability* has | *medium* | Relevance |

Table 13 describes the exhaustive list of thirty-one emergent conditions. Emergent conditions, within this case, are risk factors that entail a strategic action, process, or event meant to disturb the system operations negatively. The safety factors vary as strategic safety mechanisms account for the harm a risk factor causes operations. For example, a risk factor associated with the smart parking lot system case will be *e.10 – Low Environmental Temperature* this risk violates requirement seven, which requires that the central computing system be able to operate in high temperatures but doesn't require the central computing system to be able to operate in conditions lower than freezing point 0 degrees Celsius therefore causing this to be systematic risk. On the other hand, safety factors such as the implementation of *e.21 - Geofencing technology* contribute to safety by enforcing zonal restrictions that align with *requirements 26 & 27.*

**TABLE 13. Emergent conditions create a set of risk and safety factors for developing a smart parking lot system. Risk and safety factors are accumulated from various sources, such as Ismagilova et al. (2022), which represent emergent conditions.**

| Index | Emergent Condition |
|---|---|
| *er.01* | Device rooting/jailbreak |
| *er.02* | Insecure authentication data, malware |
| *er.03* | Insufficient transport layer protection |
| *er.04* | Client-side injection |
| *er.05* | Security misconfiguration |

| | |
|---|---|
| *er.06* | Inadequate logging and monitoring |
| *er.07* | Sensitive data exposure |
| *er.08* | Reverse engineering |
| *er.09* | Inefficient space utilization |
| *er.10* | High Environmental temperature |
| *er.11* | Low Environmental temperature |
| *er.12* | Insufficient database size |
| *er.13* | Privacy breaches |
| *er.14* | Regulatory penalties |
| *er.15* | Overcharging |
| *er.16* | Inability to pay with a foreign payment method |
| *er.17* | Network attacks |
| *er.18* | Refuse reservation |
| *er.19* | Zonal Restriction Violations |
| *es.20* | Multi-Factor Authentication |
| *es.21* | Geofencing Technology |
| *es.22* | Currency Conversion |
| *es.23* | Thermal Sensors |
| *es.24* | Climate Control Systems |
| *es.25* | Firewall |
| *es.26* | Obfuscation Techniques |
| *es.27* | Vehicle Theft |
| *es.28* | Police Presence |
| *es.29* | Backup Generator |
| *es.30* | Smart parking sensors |
| *es.31* | Encryption Algorithms |

**TABLE 14. The grouping of emergent conditions within scenarios for the Smart Parking Lot System**

| Index | Scenarios | Emergent Conditions |
|---|---|---|
| s.01 | Cyber Security | er.01 – Device rooting/jailbreak<br>er.02 – Insecure authentication data<br>er.03 – Technological limitations<br>er.04 – Client -Side Injection<br>es.17 – Fire Suppression System<br>es.25 – Network Attacks<br>es.31 – Encryption Algorithms |
| s.02 | Environmental | er.09 – Inefficient space utilization<br>er.10 – High Environmental Temperature<br>er.11 – Low Environmental Temperature<br>es.23 – Thermal Sensors<br>es.25 – Climate Control System |
| s.03 | Compliance + Privacy | er.13 – Privacy Breaches<br>er.14 – Regulatory Penalties<br>er.19 – Zonal Restriction<br>er.18 – Refuse Reservation |
| s.04 | Operational | er.08 – Ensuring consistency of fuel property<br>es.22 – Treating and recycling waste<br>es.23 – Fire suppression systems<br>es.25 – Emergency response and spill control plans<br>es.26 – Environmental Compliance |

| | | |
|---|---|---|
| s.05 | Technological Advancements | es.21 – Geofencing Technology<br>es.30 – Smart Parking Sensors<br>es.29 – Backup Generator<br>es.26 – Obfuscation Technique<br>es.20 – Multi-Factor Authentication |
| s.06 | Security and Theft Prevention | er.27 – Vehicle Theft<br>es.28 – Police Presence<br>es.25 – Firewall<br>es.26 – Obfuscation Technique |
| s.07 | System Resilience and Preparedness | es.29 – Backup Generator<br>es.30 – Smart parking sensors<br>er.18 – Refuse reservation<br>er.08 – Reverse Engineering |

Table 14 describes seven scenarios identified by grouping one or more emergent conditions. For example, s. 21—Geofencing Technology and s. 30—Smart Parking Sensors are grouped under s.05—*Technological Advancement.* The disruptive scenarios listed can be organized as a list of all safety factors, all risk factors, or a combination of risk and safety factors.

**TABLE 15. The criteria-initiative assessment describes how well each initiative addresses the success criteria for system development of the Smart Parking Lot System when a vehicle enters the parking lot. Strongly agree is represented by a filled circle (●), *agree* is represented by a half-filled circle (◐), *somewhat agree* is represented by an unfilled circle (○), and *neutral* is represented by a dash (**

**TABLE 16. The criteria-initiative assessment describes how well each initiative addresses the success criteria for developing a Smart Parking Lot System for the case of an *Exit Parking Lot.* Strongly agree is represented by a filled circle (●), *agree* is represented by a half-filled circle (◐), *somewhat agree* is represented by an unfilled circle (○), and *neutral* is represented by a dash (**

Table 15 describes a criteria initiative assessment for action. The criteria initiative assessment scores are generated from the consensus literature review. For example, according to the table above, the initiative *x.01 – Drive to lot entrance*, *somewhat agrees* with the criteria *c.05 - Environmental* (Biyik et al., 2021; Barriga et al., 2019; Zhu et al., 2021). Table 16 describes the criteria-initiative assessment for reserving a parking slot using the parking application. For example, *x.20 – agrees* with the criteria *c.01- Reduction of Traffic.* Table 17 refers to a criteria-initiative assessment. Table 18 describes the criteria-scenario relevance assessment for developing a smart parking lot system. For example, scenario *s.01 – Cyber Security decreases somewhat (DS) criterion c.05 - Environmental* goals.

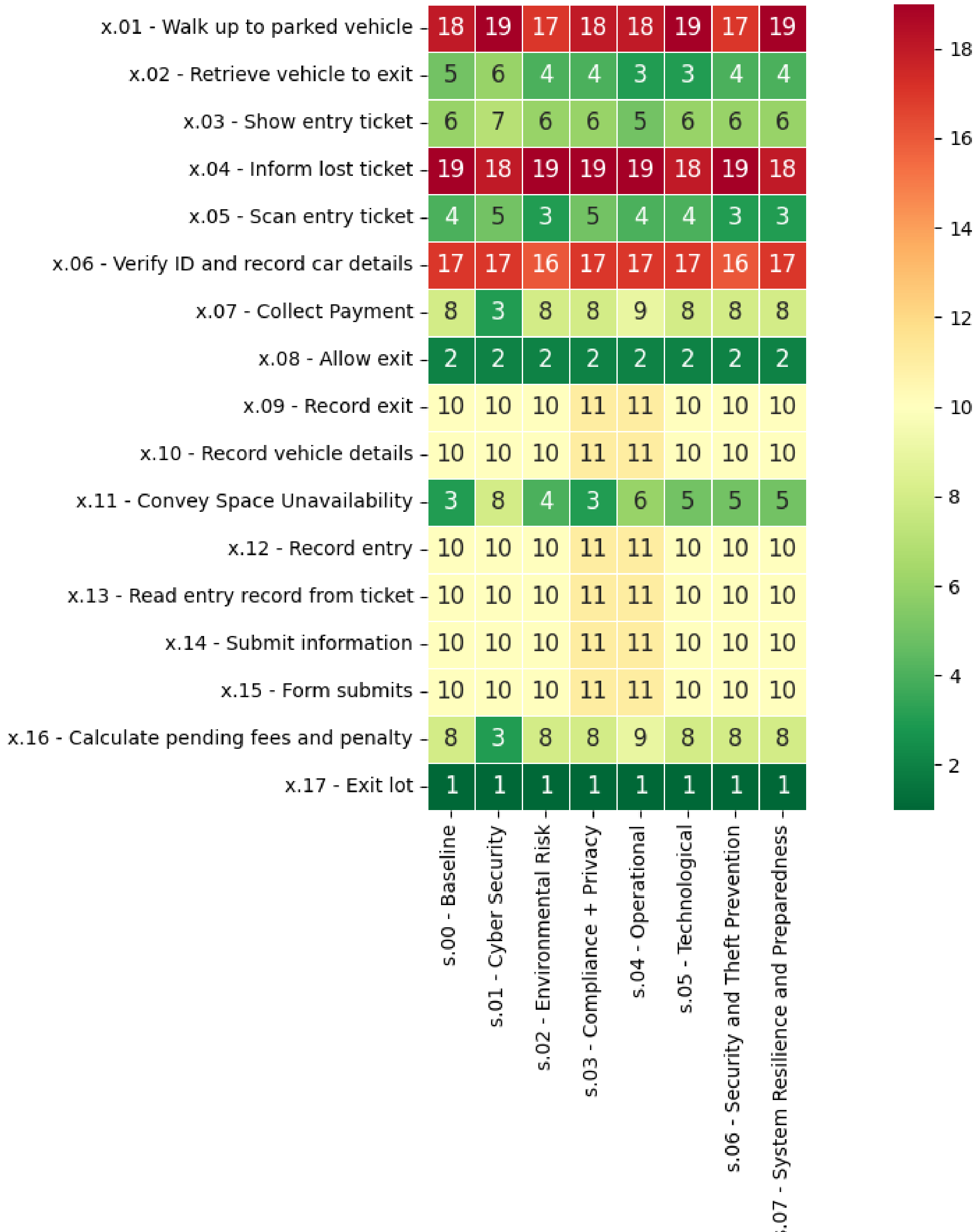
**TABLE 18. Reweighting of criteria under each scenario from the perspective of various Smart Parking Lot systems. *Decreases Somewhat* = DS, *Decreases* = D, *Somewhat Increase = SI, Increases = I.***

| Index | *s.01* | *s.02* | *s.03* | *s.04* | *s.05* | *s.06* | *s.07* |
|---|---|---|---|---|---|---|---|
| *c.01* | - | - | I | I | I | - | I |
| *c.02* | - | I | IS | - | IS | I | IS |
| *c.03* | - | I | I | - | IS | I | I |
| *c.04* | I | DS | IS | - | I | DS | I |
| *c.05* | DS | - | I | - | IS | - | IS |
| *c.06* | D | DS | - | I | IS | - | IS |
| *c.07* | - | DS | D | I | IS | DS | I |

**TABLE 19. Initiative-scenario ranking chart. This table describes the ranking of each scenario for entering a smart parking lot.**

| | s.00 - Baseline | s.01 - Cyber Security | s.02 - Environmental Risk | s.03 - Compliance + Privacy | s.04 - Operational | s.05 - Technological | s.06 - Security and Theft Prevention | s.07 - System Resilience and Preparedness |
|---|---|---|---|---|---|---|---|---|
| x.01 - Drive to lot entrance | 7 | 4 | 3 | 6 | 10 | 7 | 5 | 7 |
| x.02 - Show reservation confirmation | 4 | 3 | 2 | 2 | 5 | 3 | 3 | 4 |
| x.03 - Request on the Spot Entry | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 |
| x.04 - Enter lot to park | 5 | 8 | 7 | 7 | 4 | 5 | 7 | 5 |
| x.05 - Leave Parking Lot | 11 | 1 | 11 | 8 | 11 | 11 | 11 | 11 |
| x.06 - Perform security check on vehicle | 16 | 14 | 16 | 16 | 16 | 16 | 16 | 16 |
| x.07 - Scan reservation confirmation | 6 | 6 | 5 | 5 | 6 | 5 | 4 | 6 |
| x.08 - Convey refused reservation | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 |
| x.09 - Allow entry and provide slot/level info | 2 | 7 | 6 | 4 | 1 | 3 | 6 | 3 |
| x.10 - Record vehicle details | 16 | 14 | 16 | 16 | 16 | 16 | 16 | 16 |
| x.11 - Convey Space Unavailability | 14 | 18 | 14 | 15 | 14 | 14 | 14 | 15 |
| x.12 - Record Entry | 16 | 14 | 16 | 16 | 16 | 16 | 16 | 16 |
| x.13 - Form Submit | 13 | 13 | 13 | 13 | 13 | 13 | 13 | 13 |
| x.14 - Display Slot Unavailability | 14 | 18 | 14 | 14 | 14 | 14 | 15 | 14 |
| x.15 - Display Slot Assignment | 2 | 5 | 4 | 3 | 3 | 2 | 2 | 2 |
| x.16 - Submit details | 8 | 9 | 8 | 9 | 7 | 8 | 8 | 8 |
| x.17 - Display Refusal | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 |
| x.18 - Read Reservation Confirmation | 8 | 9 | 8 | 9 | 7 | 8 | 8 | 8 |
| x.19 - Slot Assignment | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 1 |
| x.20 - Check Reservation Validity | 8 | 9 | 8 | 9 | 7 | 8 | 8 | 8 |
| x.21 - Record Entry | 16 | 14 | 16 | 16 | 16 | 16 | 16 | 16 |

**TABLE 20. Initiative-scenario ranking chart. This table describes the ranking of each scenario for retrieving a vehicle.**



| | s.00 - Baseline | s.01 - Cyber Security | s.02 - Environmental Risk | s.03 - Compliance + Privacy | s.04 - Operational | s.05 - Technological | s.06 - Security and Theft Prevention | s.07 - System Resilience and Preparedness |
|---|---|---|---|---|---|---|---|---|
| x.01 - Walk up to parked vehicle | 18 | 19 | 17 | 18 | 18 | 19 | 17 | 19 |
| x.02 - Retrieve vehicle to exit | 5 | 6 | 4 | 4 | 3 | 3 | 4 | 4 |
| x.03 - Show entry ticket | 6 | 7 | 6 | 6 | 5 | 6 | 6 | 6 |
| x.04 - Inform lost ticket | 19 | 18 | 19 | 19 | 19 | 18 | 19 | 18 |
| x.05 - Scan entry ticket | 4 | 5 | 3 | 5 | 4 | 4 | 3 | 3 |
| x.06 - Verify ID and record car details | 17 | 17 | 16 | 17 | 17 | 17 | 16 | 17 |
| x.07 - Collect Payment | 8 | 3 | 8 | 8 | 9 | 8 | 8 | 8 |
| x.08 - Allow exit | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| x.09 - Record exit | 10 | 10 | 10 | 11 | 11 | 10 | 10 | 10 |
| x.10 - Record vehicle details | 10 | 10 | 10 | 11 | 11 | 10 | 10 | 10 |
| x.11 - Convey Space Unavailability | 3 | 8 | 4 | 3 | 6 | 5 | 5 | 5 |
| x.12 - Record entry | 10 | 10 | 10 | 11 | 11 | 10 | 10 | 10 |
| x.13 - Read entry record from ticket | 10 | 10 | 10 | 11 | 11 | 10 | 10 | 10 |
| x.14 - Submit information | 10 | 10 | 10 | 11 | 11 | 10 | 10 | 10 |
| x.15 - Form submits | 10 | 10 | 10 | 11 | 11 | 10 | 10 | 10 |
| x.16 - Calculate pending fees and penalty | 8 | 3 | 8 | 8 | 9 | 8 | 8 | 8 |
| x.17 - Exit lot | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |



**TABLE 21. Initiative-scenario ranking chart. This table describes the ranking of each scenario for the case of using the parking application to reserve a parking space.**

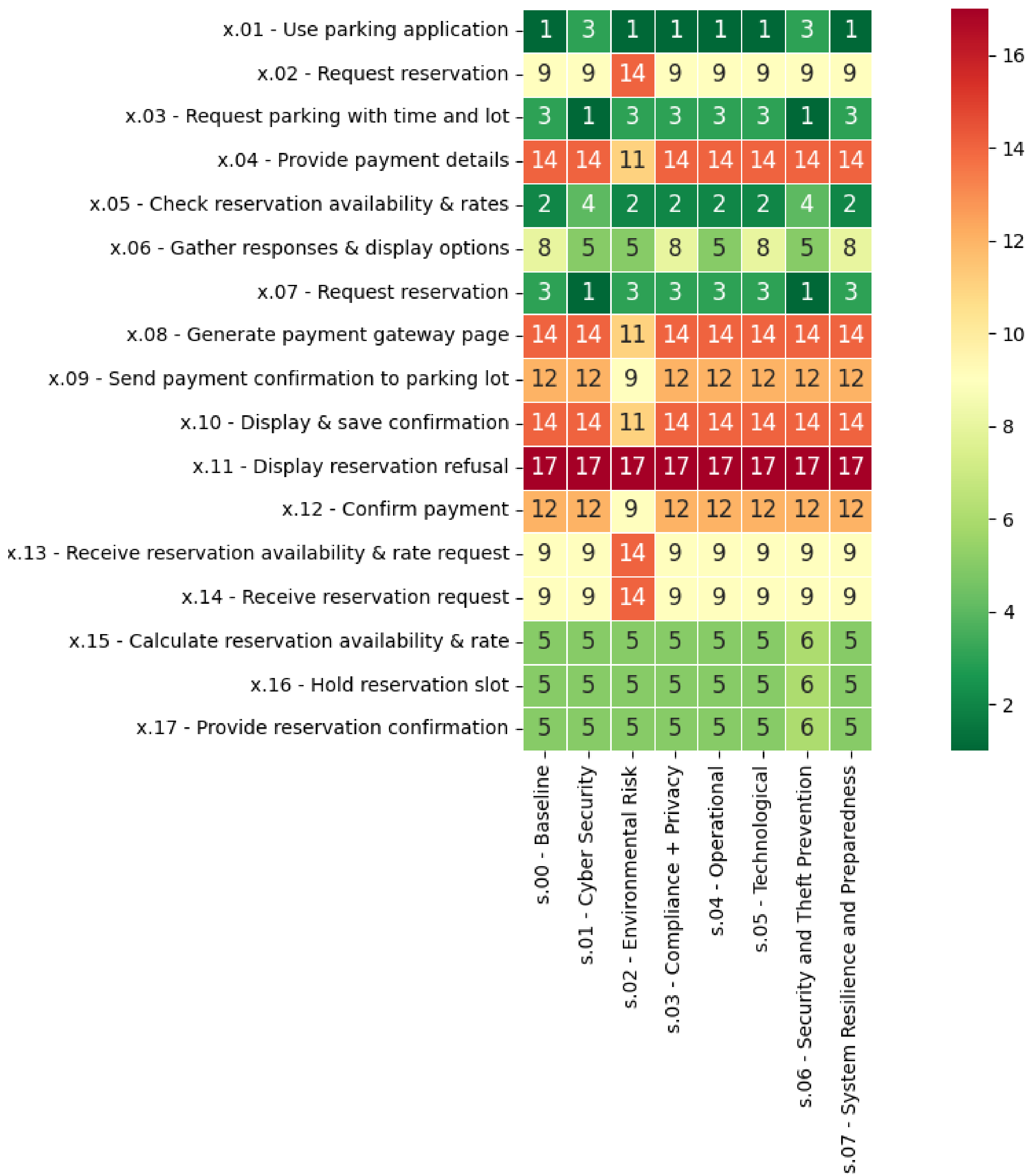

x.01 - Use parking application
x.02 - Request reservation
x.03 - Request parking with time and lot
x.04 - Provide payment details
x.05 - Check reservation availability & rates
x.06 - Gather responses & display options
x.07 - Request reservation
x.08 - Generate payment gateway page
x.09 - Send payment confirmation to parking lot
x.10 - Display & save confirmation
x.11 - Display reservation refusal
x.12 - Confirm payment
x.13 - Receive reservation availability & rate request
x.14 - Receive reservation request
x.15 - Calculate reservation availability & rate
x.16 - Hold reservation slot
x.17 - Provide reservation confirmation
1 3 1 1 1 1 3 1
9 9 14 9 9 9 9 9
3 1 3 3 3 3 1 3
14 14 11 14 14 14 14 14
2 4 2 2 2 2 4 2
8 5 5 8 5 8 5 8
3 1 3 3 3 3 1 3
14 14 11 14 14 14 14 14
12 12 9 12 12 12 12 12
14 14 11 14 14 14 14 14
17 17 17 17 17 17 17 17
12 12 9 12 12 12 12 12
9 9 14 9 9 9 9 9
9 9 14 9 9 9 9 9
5 5 5 5 5 5 6 5
5 5 5 5 5 5 6 5
5 5 5 5 5 5 6 5
s.00 - Baseline
s.01 - Cyber Security
s.02 - Environmental Risk
s.03 - Compliance + Privacy
s.04 - Operational
s.05 - Technological
s.06 - Security and Theft Prevention
s.07 - System Resilience and Preparedness
16
14
12
10
8
6
4
2

Table 19 – 21 describes the initiative scenarios that were ranked. The table outlines the ranking of each initiative under each scenario for the three individual functional architectures, focusing on the roles a driver may have in the smart parking lot system. This user-centric information is used for the mathematical framework.

## *4.3. Results*

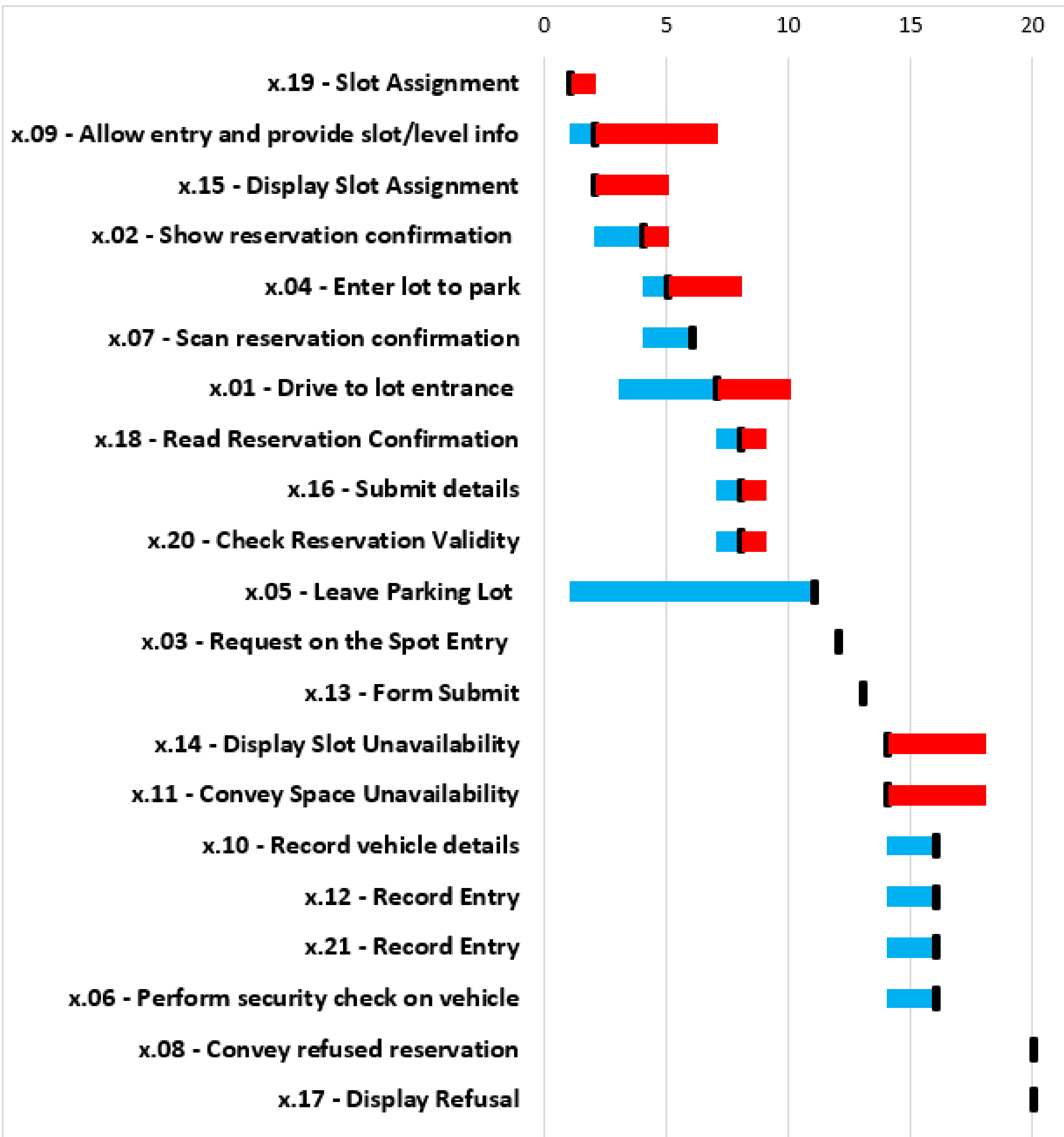


**FIGURE 17. Distributions of initiatives for functional architecture related to entering a parking lot influence ranking. The blue color signifies a promotion in ranking, indicating a positive impact on the system. In contrast, the red color denotes a demotion in ranking, suggesting a negative impact on the system. This information is crucial for understanding the risk and safety factors in the system development of the Smart Parking Lot System.**

Figure 17 describes the baseline ranking of various functions and the impact of different scenarios on the system's order and importance. The functions such as *x.19 – Slot Assignment*, *x.09 – Allow entry and provide slot/level info*, *x.15 – Display Slot Assignment*, and *x.02 – Show reservation confirmation* are identified as the most robust initiatives. Conversely, functions like *x.17 – Display Refusal*, *x.08 – Convey refused reservation*, *x.21 – Record Entry*, *x.12 – Record Entry*, *x.10 – Record vehicle details*, and *x.06 – Perform security check on vehicle* are considered the least robust initiatives. This highlights the varying degrees of resilience and importance among the different functions in the system.

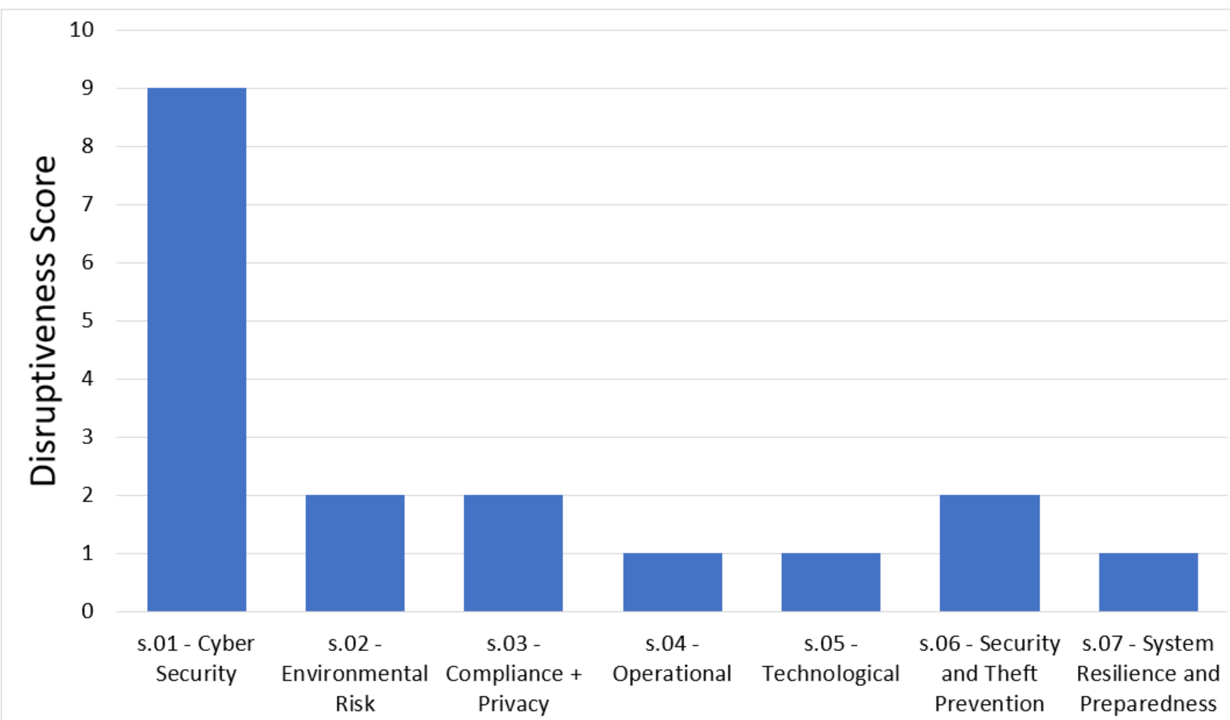



**FIGURE 18. The disruptiveness score of scenarios is based on the sum of squared differences in the priority of initiatives relative to the baseline scenario for the system development of the Smart Parking Lot System. These are the critical scenarios where the risk and safety factors may disrupt the order of initiatives. The disruptive bar graph is representative of the case of a driver entering the parking lot.**

Figure 18 describes the disruptiveness score for seven scenarios. Notably, scenario s.01—Cyber Security stands out with the highest disruptive score, underscoring its potential to significantly impact the Smart Parking Lot System. Conversely, s.04—Operational, s.05—Technological, and s.07—System Resilience and Preparedness are ranked as the least disruptive scenarios, indicating their influence on system order is less pronounced in this study.

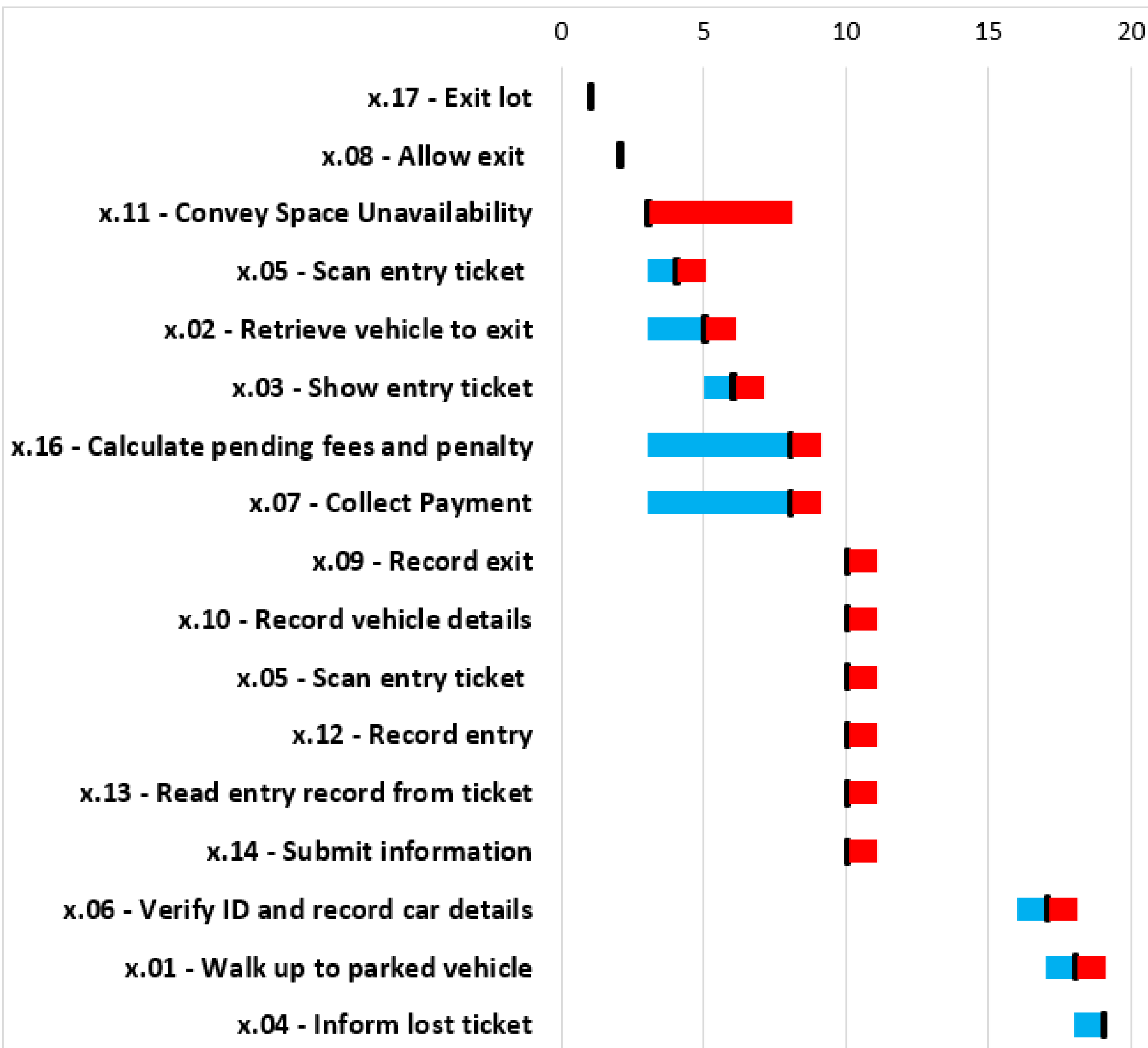



**FIGURE 19. Distribution of initiatives for the functional architecture related to a driver retrieving vehicles and exiting the parking lot, showing the influence of rankings based on potential risk and safety factors in**

**developing the Smart Parking Lot System. Blue indicates a promotion in ranking, while red indicates a demotion in ranking.**

Figure 19 provides a visual representation of the baseline ranking of various functions and the effects of multiple scenarios on their importance and order within the system. The functions designated as x.17 - Exit lot and x.08 - Allow exit to demonstrate the highest levels of resilience and robustness, indicating they are least affected by changing scenarios. On the other hand, x.11 - Convey space unavailability, x.05 -scan entry ticket, x.02 - retrieve vehicle to exit, and x.03 - show entry ticket is reasonably robust, maintaining their significance in various scenarios.

When exposed to different scenarios, these functions exhibit significant changes in their importance and ranking, underscoring their vulnerability and crucial role in the system's operation. This figure helps identify areas needing more attention to improve system robustness and reliability under various conditions by highlighting the varying degrees of resilience among the multiple functions.

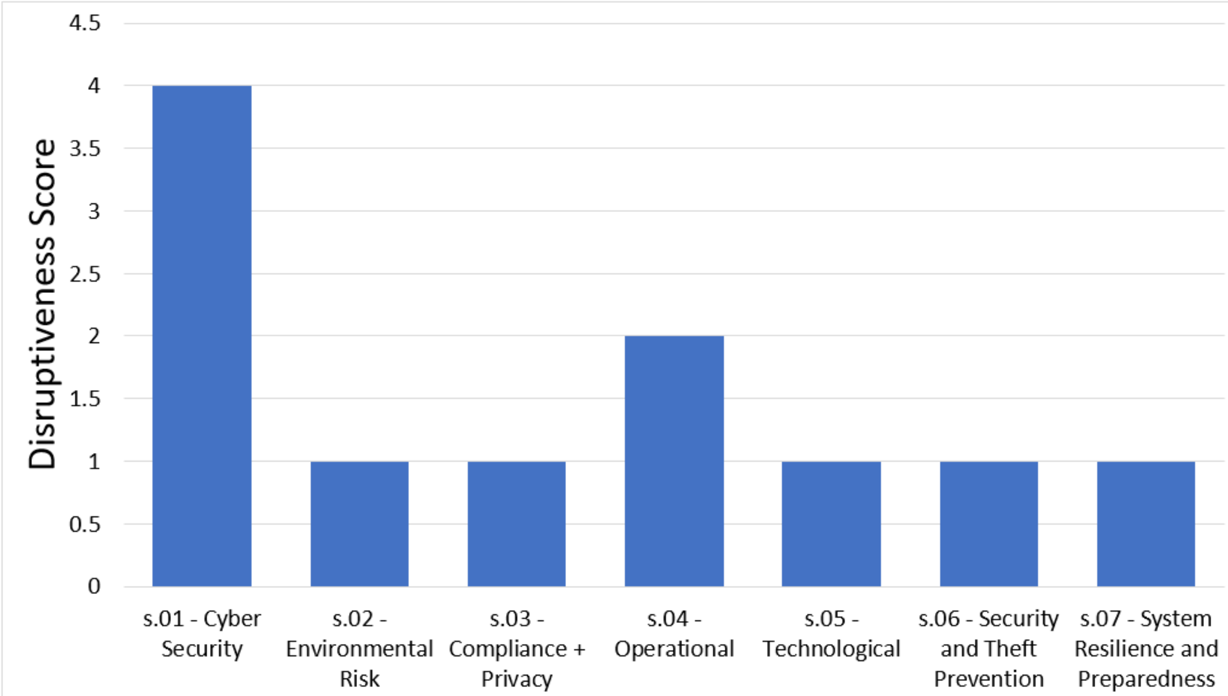



**FIGURE 20. Disruptiveness score for the case of a driver exiting the smart parking lot.**

Figure 20 illustrates the disruptiveness scores for various scenarios, highlighting the relative impact of each scenario on the system. The scenarios are ranked based on their disruptiveness scores, with higher scores indicating greater potential for disruption. *s.01 - Cyber Security* has the highest disruptiveness score of 4, indicating that issues related to cyber security have the most significant potential to disrupt the system. *s.04 - Operational* follows with a disruptiveness score of around 2, showing that operational challenges pose a considerable risk to the system's stability. *s.02 - Environmental Risk* and *s.03 - Compliance + Privacy* both have lower disruptiveness scores, around 1, suggesting these scenarios moderately impact the system. s.05 - *Technological*, *s.06 - Security and Theft Prevention*, and *s.07 - System Resilience and Preparedness* all have similar, lower disruptiveness scores, indicating these areas are less likely to cause significant disruption than Cyber Security and Operational issues. This figure emphasizes the importance of prioritizing cyber security and operational robustness to mitigate potential disruptions effectively.

The implications for tracking risk and safety factors within the functional and logical architecture of a Smart Parking Lot System. Integrating SysML with the multi-criteria impact analysis to aid in identifying critical areas where risk safety factors are to ensure robustness and reliability. The purpose of this case is to identify high-risk areas. For example, cybersecurity poses the highest disruptiveness score, which indicates that functions associated with data handling, user authentication, and network security are critical and need rigorous Safety mechanisms such as encryption algorithms or multi-factor authentication. Operational disruption functions such as slot assignment and entry validation are essential and should be designed for high efficiency. Implementing geofencing technology mitigates operation risk and enhances performance.

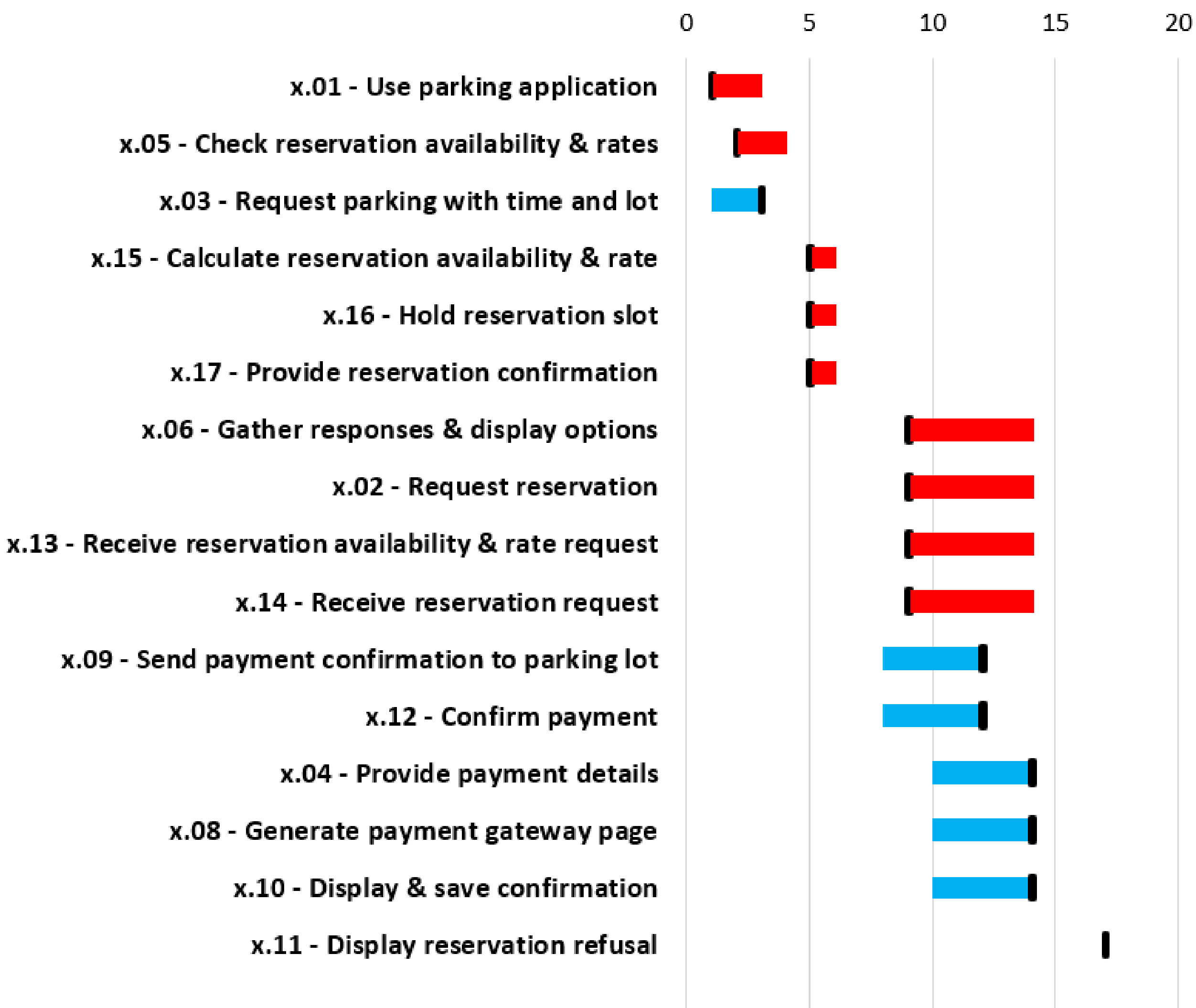



**FIGURE 21. Distributions of initiatives influence rankings based on which risk and safety factors could arise more often or do not occur during the system development for a Smart Parking Lot. Blue is a connotation for a promotion, and red is a connotation for demotion ranking.**

Based on the tables above, Figure 21 illustrates the findings from a case study that examines the baseline ordering of seventeen initiatives by a system's functional, logical architecture. Within the figure, the black bar is denoted as the baseline ranking. The bar again indicates that the function rose in priority, and the red bar represents the function declining in priority. Within this case, the top six initiatives are *x.01 - Use Parking Lot Application*, *x.05 - Check Reservation availability* *rates*, *x.03 – Request parking with time and lot*, *x.15 – Calculate reservation availability and rates*, *x.16 – Hold reservation slot*, *x.17 – Provide reservation confirmation*.

The least robust initiative is *x.11 - Display reservation refusal, x.10 - Display and save confirmation, x.08 – Generate payment gateway page, x.04-Provide Payment Details.*

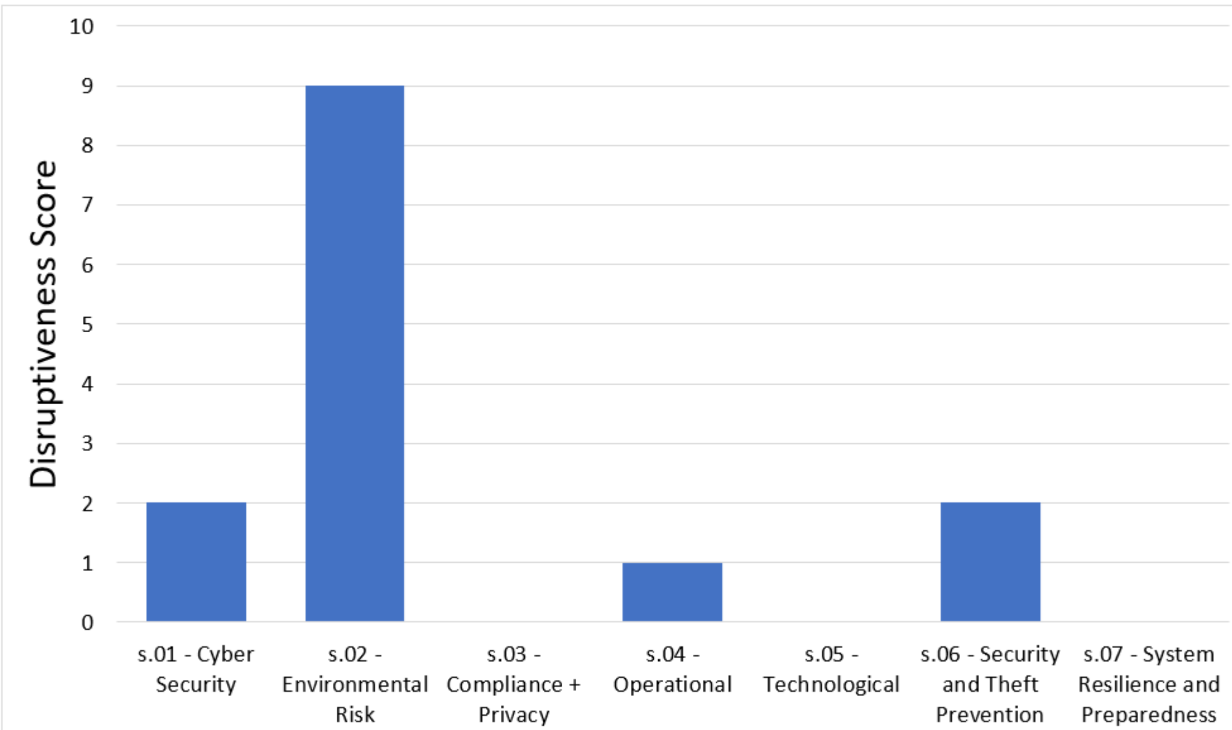



**FIGURE 22. The disruptiveness score of scenarios is based on the sum of squared differences in the priority of initiatives relative to the baseline scenario for the system development of the Smart Parking Lot System. These are the critical scenarios where the risk and safety factors may disrupt the order of initiatives. The disruptive bar graph represents the case for entering a smart parking lot.**

In this section, we explore how various scenarios impact the system's order and examine the role of the logical and functional architecture in shaping priority decisions. Figure 22 presents the disruptiveness scores for each scenario, with values normalized to a maximum of 100. Notably, three scenarios—*s.03- Compliance + Privacy*, *s.05 – Technological* and *s.07 – System Resilience and Preparedness* —register a disruptiveness score 0. Scenarios such as *s.01 – Cyber Security*, *s.04 – Operational,* and *s.06 – Security and Theft Prevention* have relatively low scores ranging from minimum to one to two, indicating minor levels of disruption on the normalized scale. This suggests that these scenarios do not substantially alter the functional activities related to the Smart Parking Lot System. Conversely, scenario *s.02—Environmental* shows significantly higher disruptiveness, indicating its potential to reorder system initiatives within the architecture significantly.

## *4.4. Summary*

This chapter outlines a framework for identifying risk and safety factors through the development of a smart parking lot system. The study describes the concept of operations in the table, which identifies seven stakeholders with various capabilities to establish the smart parking lot system. This chapter identifies six criteria, twenty-two requirements, and three different sets of initiatives representing the individual scenarios for interacting with a smart parking lot system. The chapter envisions the functional architecture for all three cases and the logical architecture.

# Chapter 5 | Case Study for Sustainable Aviation Fuels Supply Chain

## *5.1. Introduction*

This chapter describes applying a framework used to understand how system order disrupts system development for the supply chain for Sustainable Aviation Fuel (SAF). The motivation for the study is described below.

The transition from traditional fuels to more sustainable alternatives is crucial for the future of both ground and air transportation. While ground vehicles can transition to electric and hydrogen-based options, the U.S. aviation industry relies on 18 billion gallons of derived liquid jet fuel annually to support flight operations. To address the environmental impact of this dependency, SAF has been introduced as a viable alternative. SAF is a liquid drop-in fuel compatible with existing fuel systems and infrastructure, facilitating a smoother transition towards greener aviation practices.

In alignment with national decarbonization goals, various government-led initiatives have been launched, such as the SAF Grand Challenges of 2021, the Aviation Climate Action Plan (ACAP), the Farmers to Fly Act, and SAF tax credits. These initiatives combine technological innovation, policy support, and economic incentives to reduce greenhouse gas (GHG) emissions and enhance the environmental performance of the aviation sector on a global scale (Federal Aviation Administration, 2021; U.S. Department of Energy; United States, 2023; Treasury Department, IRS, 2022).

Understanding the supply chain processes during the conceptual phase is essential to establish a robust foundation for SAF deployment. However, current methodologies often overlook critical risk and safety factors that can significantly impact the reliability and effectiveness of these supply chains.

This paper addresses this gap by proposing a framework for incorporating risk-safety factors into the SysML development life cycle for the SAF supply chain. The focus will be establishing a comprehensive context for the SAF supply chain and communicating it using SysML architecture. The methodology involves gathering input from stakeholders and existing literature on system criteria, concepts of operations, and system requirements. A custom SysML profile will be developed to incorporate risk and safety factors, facilitating comprehensive *criteria-initiative* and *criteria-scenario* assessments. These assessments will help rank various initiatives and identify potential disruptive scenarios.

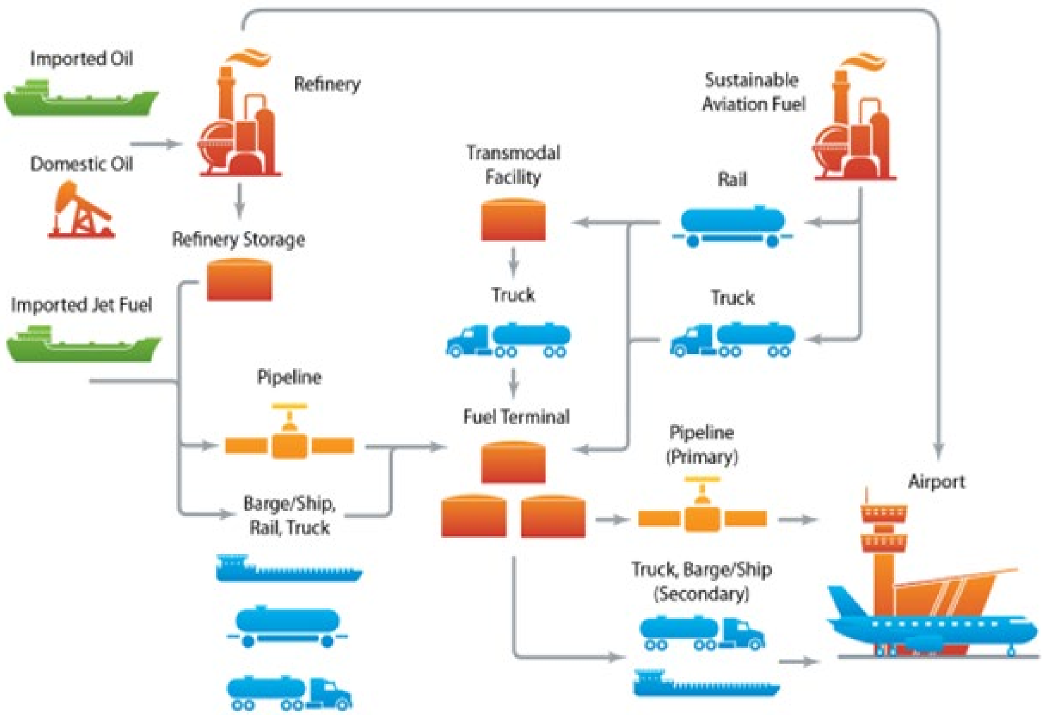



**FIGURE 23. Diagram illustrating the supply chain process for jet fuel, starting from imported and domestic oil, through refineries and various transportation modes, to the final delivery at airports. It includes the integration of sustainable aviation fuel into the supply chain.**

The development of the SAF industry consists of various phases and interactions. All phases associated with the development of the SAF industry and supply chain face uncertainties. Stakeholders involved with the supply chain such as farmers, producers, airlines, and airports have different goals, interests, concerns, and priorities. Therefore, prioritizing investment helps manage the complexities by focusing on initiatives under various future scenarios.

This chapter describes the use of a Risk-Safety Profile to acknowledge how system order is disrupted by risk and safety factors experienced within the system development for a SAF Supply Chain. The section focuses on establishing the context for the Supply chain for SAF while communicating it using SysML architecture. The approach begins by gathering stakeholders, and literature on system criteria along with the concept of operations, and initiatives alongside system requirements. The collection of risk and safety factors information will be demonstrated within the SysML custom profile. This includes a high-level design. The section will generate the C-I assessment and C-S assessment. The assessment will help us develop the ranking of the initiatives and disruptive scenarios.

## *5.2. Application of Multi-Criteria Impact Analysis on Sustainable Aviation Fuels Supply Chain*

### *5.2.1. Concept of Operations and System Criteria*

**TABLE 22. Concept of Operations regarding system supply chain for SAF.**

| Stakeholders | Capabilities |
|---|---|
| Airports | **Supply Infrastructure**<br>**Economic Benefits** |
| Airlines | **Fuel Security**<br>**Environmental Compliance**<br>**Market Competitiveness** |
| Feedstock Producers | **Developmental of Infrastructure**<br>**Security and Surveillance** |
| SAF Refineries | **Investment in Technology**<br>**Facility Siting**<br>**Market Development** |
| Policymakers and Regulators | **Supportive Legislation**<br>**Regulatory Compliance**<br>**Incentives for Development** |
| Researchers | **Research and Development**<br>**Uncertainty Analysis** |

Table 23 describes six success criteria that were identified to develop a viable supply chain for sustainable aviation fuels (SAF). These criteria align with the FAA's mission and national and international goals set by various stakeholders. Here are the criteria:

*C.01 – Production Quantity*: Refers to the supply of SAF, ensuring sufficient production to meet demand. *C.02 – Production Quality*: Refers to the quality of the SAF and how it impacts other phases of its use and production. *C.03 – Environmental Quality*: Involves greenhouse gas emissions, land use change, freshwater use, pesticides, fertilizers, and biodiversity associated with producing SAF. *C.04 – Economic Development*: Refers to the employment opportunities generated from a given SAF initiative. *C.05 – Life Cycle Cost*: Refers to the financial investment required throughout the overall lifecycle of SAF. *C.06 – Regulatory Compliance and Global Collaboration*: Involves meeting international standards, certifications, and regulations, ensuring the SAF initiatives are globally recognized and compliant.

These criteria serve as essential benchmarks to ensure that the development and implementation of SAF supply chains are sustainable, environmentally friendly, economically beneficial, and globally compliant.

**TABLE 23. Criteria used to evaluate the initiatives for regional bio jet fuel industry system development, based on the FAA's (2011) mission and vision for the future and the white house (2011) goals for energy security.**

| Index | Criterion |
|---|---|
| c.01 | Production Quantity |
| c.02 | Production Quality |
| c.03 | Environmental Quality |
| c.04 | Economic development |
| c.05 | Life-cycle cost |
| c.06 | Regulatory compliance and global collaboration |

### *5.2.2. System Initiatives and Requirements*

Table 24 describes fourteen system requirements with unique IDs. The requirement diagram represents the contained requirements. For example, "Requirement ID 1," related to the research and development of establishing a facility, is an example of a requirement used to develop the system design for SAF.

**TABLE 24. Outline of key system requirements for the SAF supply chain.**

| ID | Description | Satisfied By |
|---|---|---|
| *1* | **R&D Facility Establishments:** An R&D must be established and focus on developing crop varieties that demonstrate a minimum 20 % increase in yield over current standards. | Feedstock Cultivation and Collection |
| *2* | **Cultivation Protocol:** Cultivation protocols must be documented and implemented across all farming operations by Q1 20XX, with adherence monitored bi-annually. | |
| *3* | **Collection System Efficiency:** Collection systems must achieve 90% efficiency in biomass handling and processing, with losses not exceeding 10%, measured annually. | |
| *4* | **Supply Contract Clarity:** Supply contracts must specify feedstock quantities with a 5% variance, price fluctuation limits of no more than 10%, and quality metrics with less than 5% deviation, effect from Q1 20XX. | |
| *5* | **Workforce Development Implementation:** A workforce development program, achieving at least an 80% employment retention rate annually, shall be operational by Q2 20XX. | Feedstock Processing and Bio-Refinery |
| *6* | **Bio-refinery Siting Study:** A comprehensive siting feasibility study must be completed by Q3 20XX, assessing logistics, resource availability, and regulatory environment impact, with a 90% confidence level in site selection. | |
| *7* | **Technology Diversification:** Each bio-refinery must integrate at least two distinct refining technologies by Q2 20XX, with operational flexibility assessed and verified bi-annually. | Bio-Refinery Technology |
| *8* | **Process Efficiency Standard:** Refining processes must achieve at least 85% of the theoretical conversion efficiency, verified during annual reviews. | |
| *9* | **Blending Facility Spec:** Blending facilities must handle at least three types of biofuels and meet fuel specification standards with 95% accuracy, assessments conducted quarterly. | |
| *10* | **Pipeline Conversion Compliance:** Converted pipelines must comply with current biofuel transportation standards, with an effectiveness rate of 98%, verified through an annual inspection. | Transportation |
| *11* | **Storage Expansion Metric:** Storage facilities must expand total capacity by 20% by Q4 20XX, with utilization rates reviewed semi-annually. | Storage |
| *12* | **Market Plan:** Supply chain stakeholders shall adopt a market plan that aims at increasing biofuel | |
| *13* | **Financial Incentive Accessibility:** Financial incentives must be structured to increase stakeholder participation. | |
| *14* | **Coalition Activity Compliance:** A coalition framework that facilitates at least quarterly communications and coordinated actions must be established | |

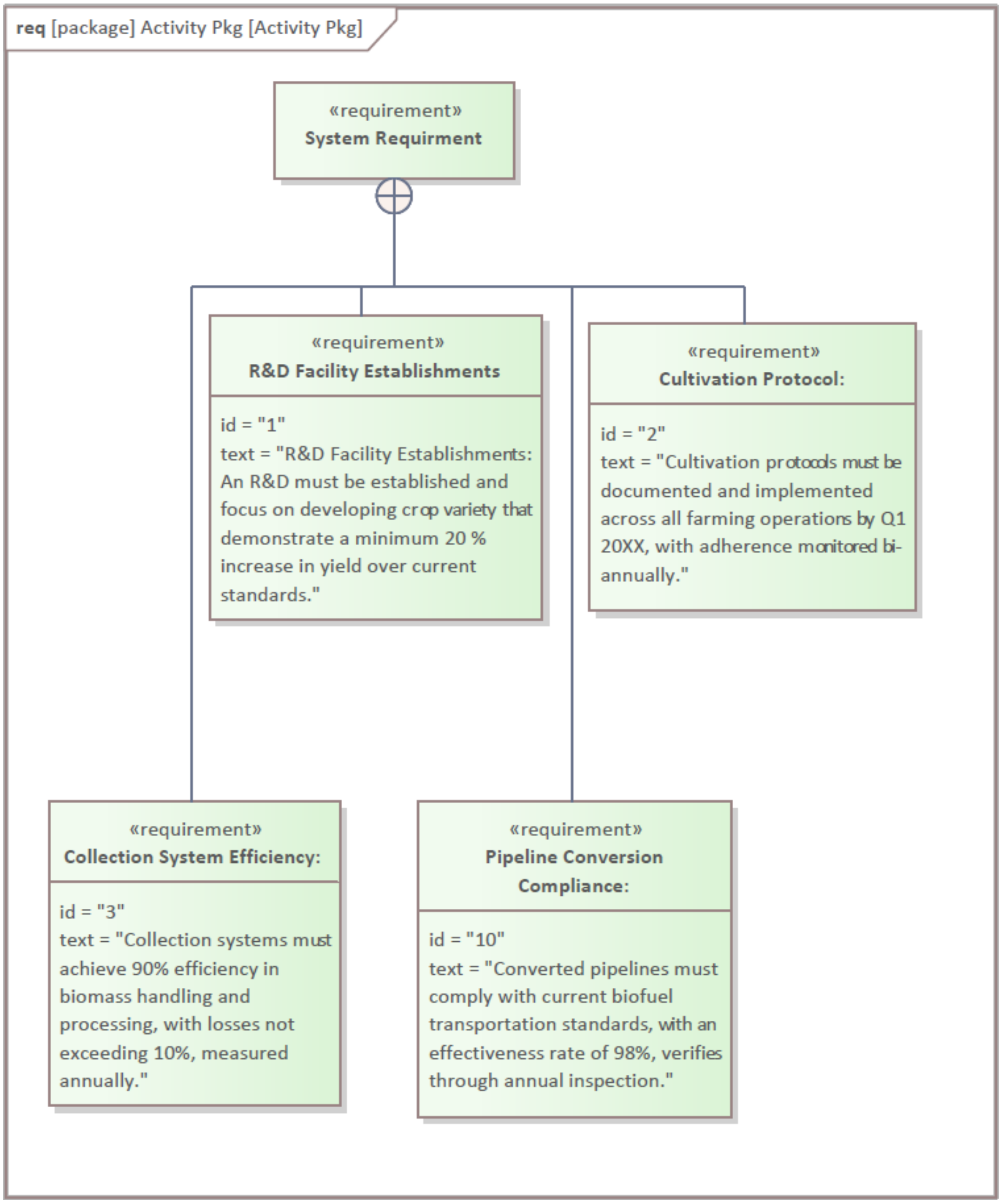



**FIGURE 24. System requirements are captured within a requirement diagram in SysML utilized for developing the functional and logical architecture.**

**TABLE 25. Initiatives for SAF supply chain development adapted from reference (Connelly et al., 2015).**

| Index | Initiatives |
|---|---|
| x.01 | Invest in R&D for productive feedstocks |
| x.02 | Cultivate oil crop feedstock |
| x.03 | Cultivate lignocellulosic feedstock |
| x.04 | Cultivate algae feedstock |
| x.05 | Cultivate halophyte feedstock |
| x.06 | Develop infrastructure for wood residue |
| x.07 | Develop infrastructure for municipal solid waste |
| x.08 | Develop infrastructure for agriculture residue |
| x.09 | Long-term contracts for feedstock supply |
| x.10 | Develop workforce |
| x.11 | Locate refineries closest proximity city or metro |
| x.12 | Locate refineries near feedstock |
| x.13 | Locate refineries near existing transport infrastructure |
| x.14 | Invest in HEFA |
| x.15 | Invest in Fischer-Tropsch |
| x.16 | Invest in Alcohol to Jet |
| x.17 | Invest in Fermentation Renewable Jet |
| x.18 | Invest Pyrolysis |
| x.19 | Convert existing petroleum pipelines for biofuel |
| x.20 | Increase storage capacity at strategic locations like airports |
| x.21 | Establish new trucking routes specifically designed for biofuels |
| x.22 | Site Blending Facilities |
| x.23 | Develop Market Co-Products |
| x.24 | Diversify Demand |
| x.25 | Provide Financial Incentives |
| x.26 | Bio-jet Fuel Purchase Agreements |
| x.27 | Co-location strategies |
| x.28 | Establish Coalitions |

Table 25 describes twenty-eight initiatives identified through a study conducted by (Connelly et al., 2015). These initiatives are characteristics and functions used to carry out system requirements mentioned in earlier systems engineering life stages. Each initiative listed belongs to a stage within the supply chain that allows for collecting feedstocks for the storage and delivery of SAF at airports. A list of initiatives is gathered from various sources, beginning with (Connelly et al., 2015), commercial aviation experts, academic researchers, and government agencies. For example, *x.01 Invest in Research and Development, x.02 Cultivate lignocellulosic feedstock, x.03 Cultivate oilseed crops as feedstock, x.04 Cultivate halophyte feedstock, and x.05 Cultivate algae as feedstock* falls in the feedstock collection phase of the supply chain are shown in the first partition of Figure 14 activity diagram in SysML.

### *5.2.3. Functional and Logical Architecture*

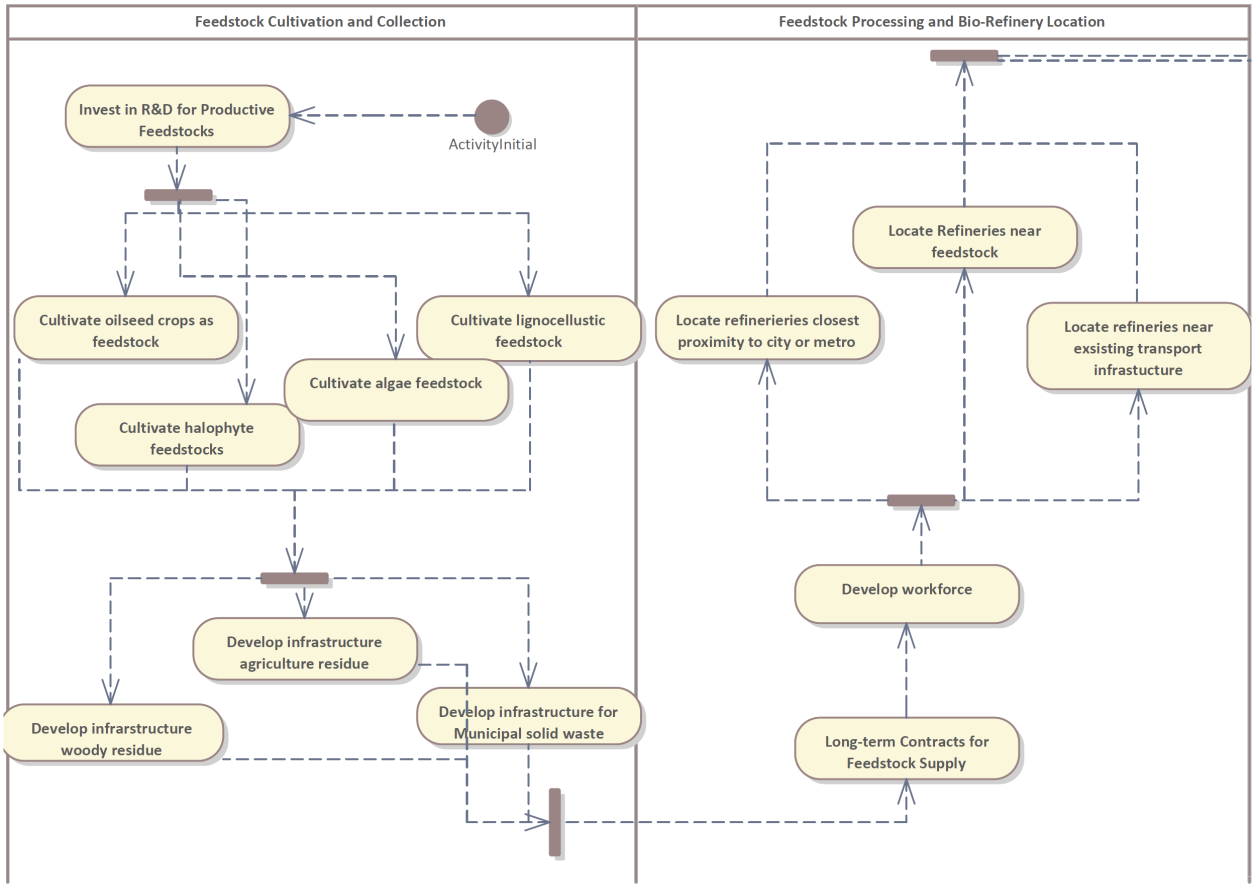



**FIGURE 25. SysML activity diagram representing the functional architecture of developing a supply chain system for the SAF parking lot system for a smart city. This activity partition describes the behavior that envisions cultivating and collecting feedstock, processing feedstock, and deciding location adapted from (Connelly et al., 2015)**

Figure 25 describes how initiatives are applied to a functional architecture. Various initiatives are identified as critical functions in the supply chain for SAF that deal with processing feedstock transportation to biorefineries. The initiatives within this swim lane of the activity diagram align with criteria representative of stakeholder objectives such as logistics and transportation cost, environmental impact, and regulatory and market considerations.

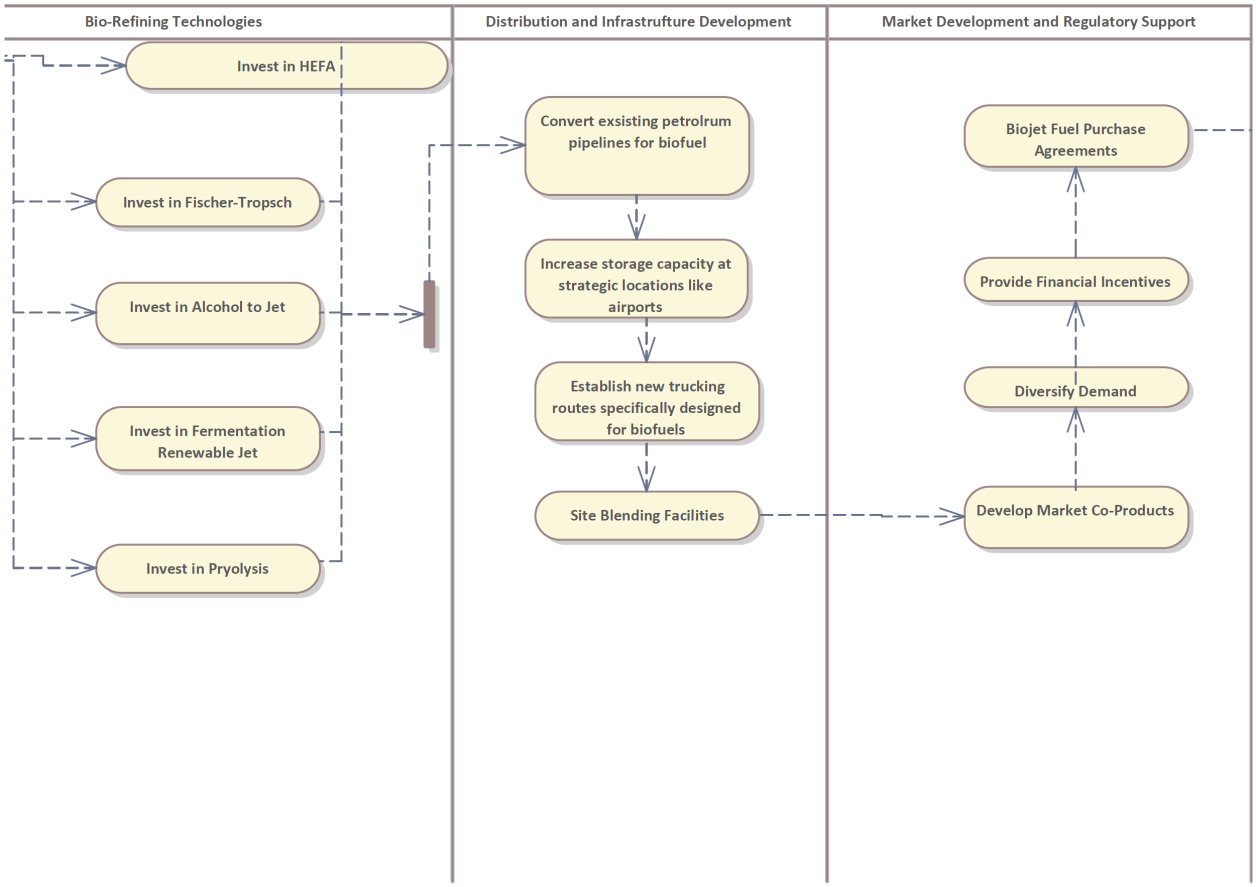



**FIGURE 26. The SysML Activity Diagram represents the functional architecture of SAF's supply chain development. This activity diagram describes the behavior that envisions bio-refinery technology, distribution, and infrastructure development and collecting market development and regulatory support (Connelly et al., 2015).**

Figure 26 represents the second half of the activity diagram shown in SysML. The swim lanes represented in this figure are associated with phases that align with the process of creating opportunities for the deployment of SAF. The forks represented by a dark-shaded vertical rectangle that follows the action are an additional attribute to indicate that it prompts parallel actions at multiple sites and activities.

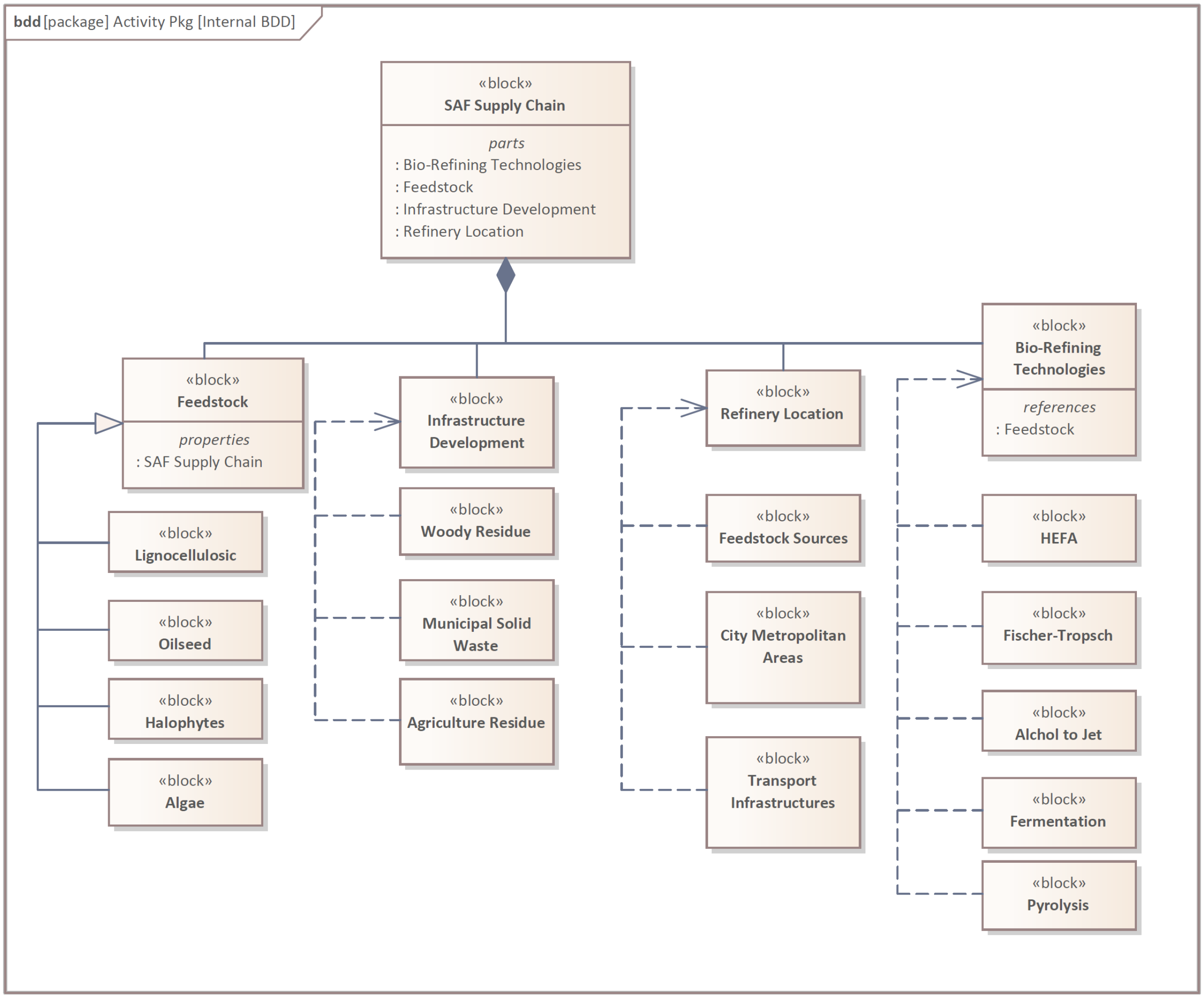



**FIGURE 27. SysML block definition diagram that illustrates the logical architecture of a Sustainable Aviation Fuel (SAF) supply chain system. It highlights various logical blocks within the system and the specific functions assigned to each block adapted from (Connelly et al., 2015).**

Figure 27 describes the high-level decomposition of the structure of the SAF supply chain within a block definition diagram. As the diagram indicates, the SAF supply chain will consist of four main subsystems: "Feedstock," Infrastructure Development, Refinery Location, and Bio-Refinery Location. This diagram is important due to its logical structure, which aids in identifying where hidden risks may be located within the system.

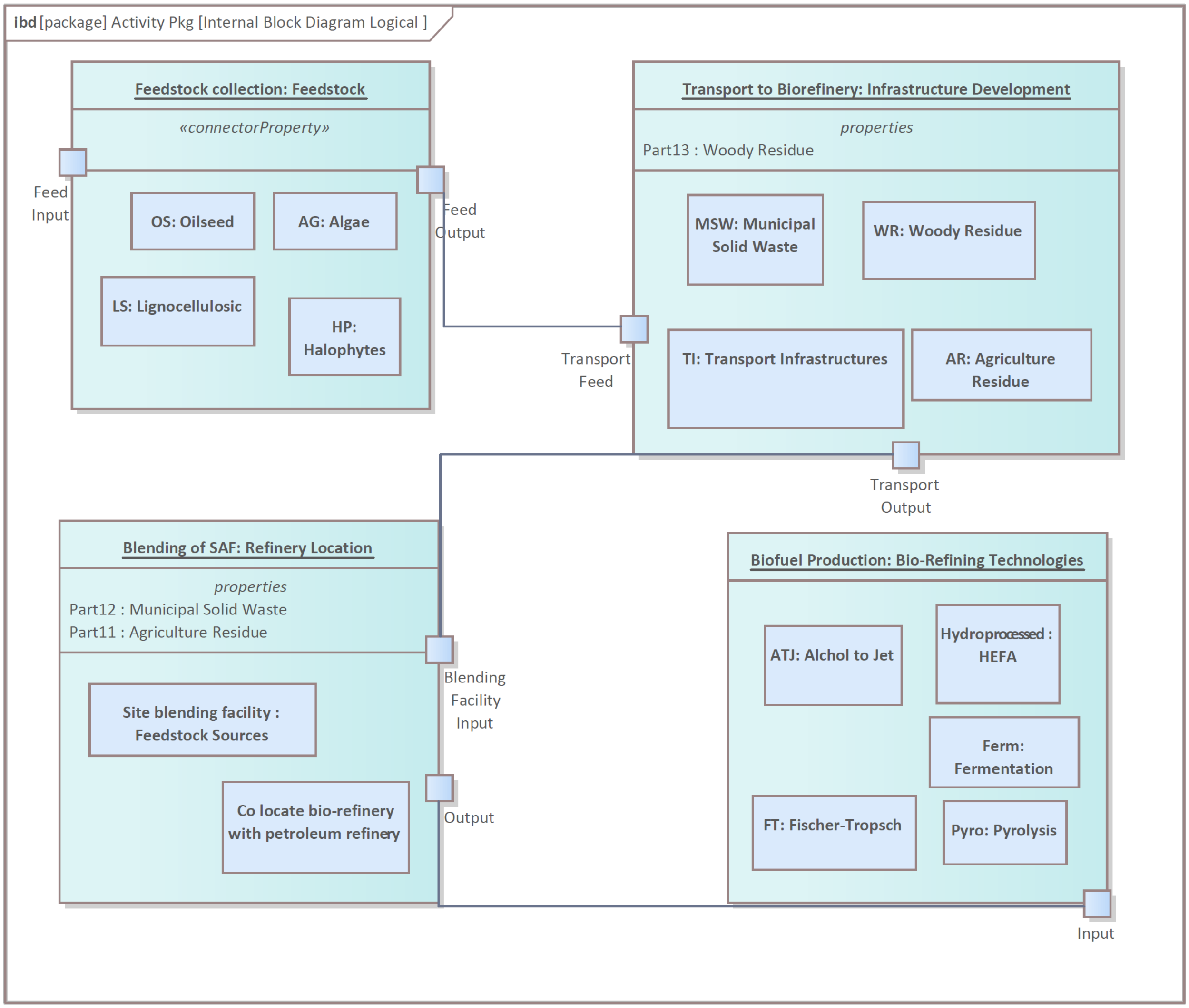



**FIGURE 28. SysML Internal Block Diagram illustrating the connections and interfaces between internal subsystems of the Sustainable Aviation Fuel (SAF) supply chain, detailing feedstock collection, transportation logistics, and bio-refining technologies.**

Figure 28 describes the internal block diagram for the internal structure of the different sources of biomass used in the supply chain, such as oilseed, algae, lignocellulosic materials, and halophytes, which are captured in this section. It shows how these various feedstocks are gathered and fed into the transportation system, emphasizing the relationships between input and output crucial for supply chain management.

This diagram shows the infrastructure and transportation required to support the biorefining processes. It describes the transportation infrastructures for various components, such as agricultural residue, woody residue, and municipal solid waste, and how these materials get to the sites of biorefining.

This block illustrates how SAF is blended at a particular refinery site. It highlights the integration of SAF production with current petroleum refining processes to leverage facilities and infrastructure. It shows the blending of agricultural residue and municipal solid waste at a site blending facility co-located with a petroleum refinery.

The diagram's last section explains the different biorefining techniques employed to turn the biomass into SAF. It encompasses pyrolysis, fermentation, Fischer-Tropsch (FT) synthesis, alcohol to jet, and HEFA (Hydroprocessed Esters and Fatty Acids). Every component is linked together to show how materials move and undergo changes to become the finished biofuel.

### *5.2.4. Applying Custom Stereotype to Functional Architecture*

Figure 29 is an example of how the stereotype risk and safety profile for a specific component within the functional architecture. The stereotypes "Risk Factor" and "Safety Factor" create a child diagram of the metaclass "Scenario". The inability to link all link block diagrams to various elements across all architectures. In this capture, the name of the risk and safety factor factors are captured using the stereotype. The element derived from the functional architecture, in this example, *Invest in HEFA,* consists of attributes. The attributes included in the elements store values associated with the criteria-initiative assessment. The innovation allows users to understand what specific risk and safety factors are associated with an action and how well does action aligns with the criteria for this system.

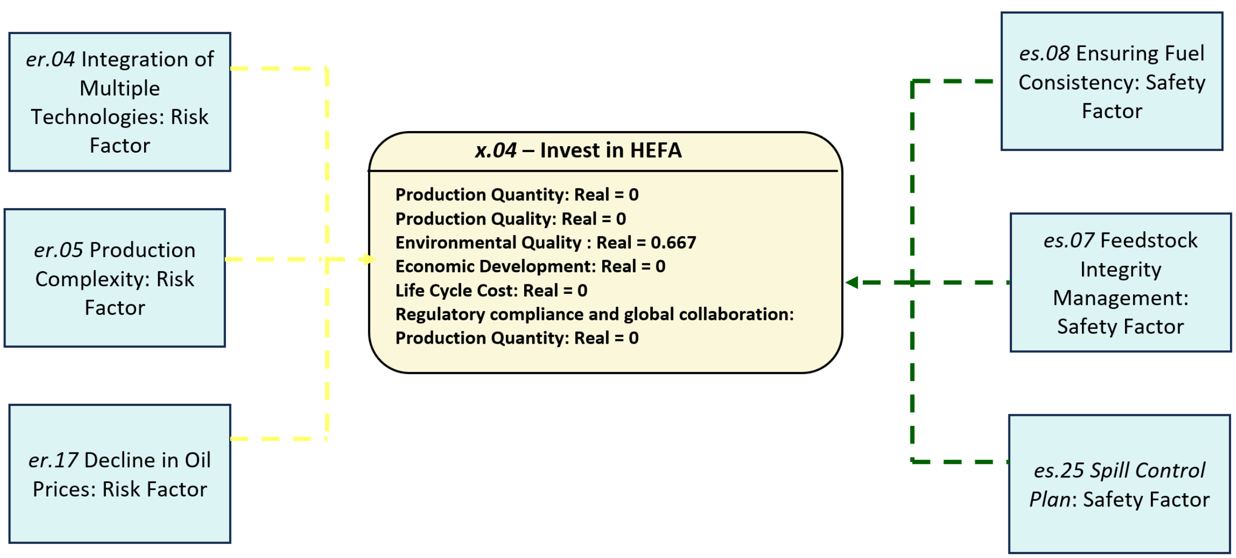



**FIGURE 29. SysML Activity Diagram represents how the risk-safety profile is applied to functions associated with the development aspects of the system architecture of a SAF supply chain. This partition of activity describes the behavior that is envisioning cultivating and collecting feedstock.**

Table 26 describes the criteria-initiative assessment for how well each initiative addresses the success criteria for the system development of the SAF supply chain. For instance, *x.01 – Invest R&D for productive feedstock* addresses the success criteria *c.02- Production quality* by using *somewhat agree* as an empty circle (○**)** and neutral for *c.03 – Environmental quality* by a dashed line (

*initiatives*. However, safety factors such as *e.19 – Diversifying Feedstock Supplier and e.23 - Fire Suppressant Systems* are safety factors and will generally positively impact production (Doliente et al., 2020; Adekitan, 2018).

**TABLE 27. Risk and safety factors from various sources represent emergent conditions (Doliente et al., 2020; Adekitan, 2018).**

| Index | Risk and Safety Factors |
|---|---|
| er.01 | Unsafe Flash Point |
| er.02 | Freezing point |
| er.03 | Combustion Heat |
| er.04 | Integration of multiple bio-refinery technology |
| es.05 | Development in Aircraft Technology |
| er.06 | Low-quality SAF technology |
| es.07 | Feedstock integrity management |
| es.08 | Ensuring consistency of fuel property |
| es.09 | Long-term contracts for feedstock supply |
| er.10 | Loss on investment |
| es.11 | Variability in feedstock quality |
| er.12 | Feedstock quality diminished |
| es.13 | SAF Policy change |
| er.14 | Technological limitations |
| e.15 | Unexpected changes in regulatory policies |
| er.16 | Adverse weather conditions |
| er.17 | Decline in Oil Prices |
| er.18 | Volatility in carbon credits |
| es.19 | Diversifying feedstock supplier |
| es.20 | Advanced inventory management system |
| es.21 | Automated monitoring systems |
| es.22 | Treating and recycling waste |
| es.23 | Fire Suppression Systems |
| es.24 | Change in regulatory framework |
| es.25 | Emergency Response and Spill Control Plans |
| es.26 | Environmental compliance |
| er.27 | Competition risk |
| e.28 | Particulate matter emission |
| e.r29 | GHG emission from transporting feedstocks |
| es.30 | Energy Intensive production |
| es.32 | High Process Yield |
| es.33 | Low Process Yield |
| es.34 | Mixing Regulations |
| es.35 | ASTM Standards |
| es.36 | Cheaper SAF Production |

Table 28 is categorized as having a *medium* relevance among the other criteria.

**TABLE 28. Baseline relevance for the supply chain of the SAF.**

| The Criterion c.xx has | s.00 – Baseline | Relevance among the other criteria |
|---|---|---|
| c.01 – *Production Quantity* has | *medium* | Relevance |
| c.02 – *Production Quality* has | *medium* | Relevance |
| c.03 – *Environmental Quality* has | *medium* | Relevance |
| c.04 – *Economic Development* has | *medium* | Relevance |
| c.05 – *Life Cycle Cost* has | *medium* | Relevance |
| c.06 – *Regulatory Compliance and Global Collaboration* has | *medium* | Relevance |

Table 29 describes five scenarios identified by grouping one or more emergent conditions. For instance, *e.23 – Fire Suppression System, e.14 – Technological limitations* and *e.04 – Integration of multiple bio-refinery technologies* are grouped under scenario *s.01 – Bio-Refinery Disruption.* Other examples are *e.13 – SAF Policy Change*, *e.15 - Unexpected Changes in Regulatory Policies,* and *e.17 - Decline Oil Prices* fall under the category *s.03 – Regulatory Dynamics*.

**TABLE 29. Scenarios developed from emergent conditions for the system development of the SAF supply chain.**

| Index | Scenarios | Emergent Conditions |
|---|---|---|
| s.01 | Bio-Refinery Disruption | es.04 – Integration of multiple bio-refinery technology<br>er.06 – Low-quality SAF technology<br>er.14 – Technological limitations<br>es.21 – Automated monitoring system<br>es.23 – Fire Suppression System |
| s.02 | Feedstock Disruption | es.07 – Feedstock integrity management<br>es.09 – Long-term contract for feedstock supply<br>es.11 – Variability in feedstock quality<br>er.12 – Feedstock quantity diminished<br>es.19 – Diversifying feedstock supplier |
| s.03 | Regulatory Dynamics | es.13 – SAF Policy Change<br>er.15 - Unexpected changes in regulatory policies<br>er.17 - Decline in oil prices<br>es.18 - Volatility in carbon credits<br>er.24 - Change in regulatory framework<br>er.27 - Competition risk |
| s.04 | Environmental Compliance | es.08 – Ensuring consistency of fuel property<br>er.22 – Treating and recycling waste |

| | | |
|---|---|---|
| | | es.23 - Fire suppression systems<br>es.25 – Emergency response and spill control plans<br>es.26 – Environmental Compliance |
| s.05 | Technological Advancements | es.04 – Integration of multiple bio-refinery technology<br>es.05- Development in Aircraft Technology<br>er.06 – Low-quality SAF technology<br>es.20 – Advance inventory management system<br>es.21 - Automated monitoring system |

Table 30 describes the criteria-scenario relevance assessment for the context of the system development for the SAF supply chain. It shows how well each scenario fits the success criterion. For example, scenario s.05—Technological Advancements, Increases (I) criterion c.01—*Production quantity*.

**TABLE 30. Reweighting of criteria under each scenario for the perspective of various SAF stakeholders. *Decreases Somewhat* = DS, *Decreases* = D, *Somewhat Increase = SI, Increases = I.***

| Index | *s.01* | *s.02* | *s.03* | *s.04* | *s.05* |
|---|---|---|---|---|---|
| *c.01* | - | - | I | I | I |
| *c.02* | - | I | IS | - | IS |
| *c.03* | - | I | I | - | IS |
| *c.04* | I | DS | IS | - | I |
| *c.05* | DS | - | I | - | IS |
| *c.06* | D | DS | - | I | IS |

Table 31 describes the ranking of each initiative under each scenario associated with the case study.

**TABLE 31. Initiative-scenario ranking chart. This table describes the ranking of each initiative under each scenario for the system development of the SAF supply chain. The green-filled cells rank higher, and the red and orange-filled cells indicate a lower ranking.**

| Index | s.01 | s.02 | s.03 | s.04 | s.05 |
|---|---|---|---|---|---|
| x.01-Invest in R&D for productive feedstocks | 25 | 14 | 16 | 16 | 14 |
| x.02-Cultivate oil crop feedstock | 13 | 17 | 10 | 10 | 6 |
| x.03-Cultivate lignocellulosic feedstock | 27 | 25 | 22 | 22 | 23 |
| x.04-Cultivate algae feedstock | 14 | 3 | 18 | 18 | 18 |
| x.05-Cultivate halophyte feedstock | 26 | 20 | 15 | 15 | 21 |
| x.06-Develop infrastructure for wood residue | 21 | 9 | 22 | 22 | 23 |
| x.07-Develop infrastructure for municipal solid waster | 28 | 27 | 28 | 28 | 23 |
| x.08-Develop infrastructure for agriculture residue | 3 | 24 | 13 | 13 | 10 |
| x.09-Long-term contracts for feedstock supply | 4 | 18 | 12 | 12 | 10 |
| x.10-Develop workforce | 1 | 21 | 7 | 7 | 3 |
| x.11-Locate refineries closes proximity city or metro | 1 | 21 | 7 | 7 | 3 |
| x.12-Locate refineries near feedstock | 5 | 23 | 10 | 10 | 13 |
| x.13-Locate refineries near existing transport infrastructure | 21 | 9 | 22 | 24 | 23 |
| x.14-Invest in HEFA | 21 | 9 | 22 | 24 | 23 |
| x.15-Invest in Fischer-Tropsch | 17 | 6 | 11 | 19 | 15 |
| x.16-Invest in Alcohol to Jet | 18 | 8 | 21 | 1 | 15 |
| x.17-Invest in Fermentation Renewable Jet | 10 | 12 | 2 | 8 | 5 |
| x.18-Invest Pyrolysis | 9 | 13 | 1 | 1 | 2 |
| x.19-Convert existing petroleum pipelines for biofuel | 11 | 15 | 4 | 6 | 7 |
| x.20-Increase storage capacity at strategic location like airports | 11 | 15 | 4 | 6 | 7 |
| x.21-Establish new trucking routes specifically design for biofuels | 19 | 7 | 20 | 20 | 18 |
| x.22-Site Blending Facilities | 16 | 5 | 9 | 18 | 12 |
| x.23-Develop Market Co-Products | 7 | 1 | 3 | 1 | 1 |
| x.24-Diversify Demand | 14 | 3 | 18 | 20 | 18 |
| x.25-Provide Financial Incentives | 6 | 28 | 27 | 28 | 28 |
| x.26-Bio jet Fuel Purchase Agreements | 8 | 2 | 4 | 9 | 9 |
| x.27-Co-location strategies | 19 | 19 | 14 | 13 | 17 |
| x.28-Establish Coalitions | 21 | 25 | 22 | 14 | 22 |

## *5.3. Results*

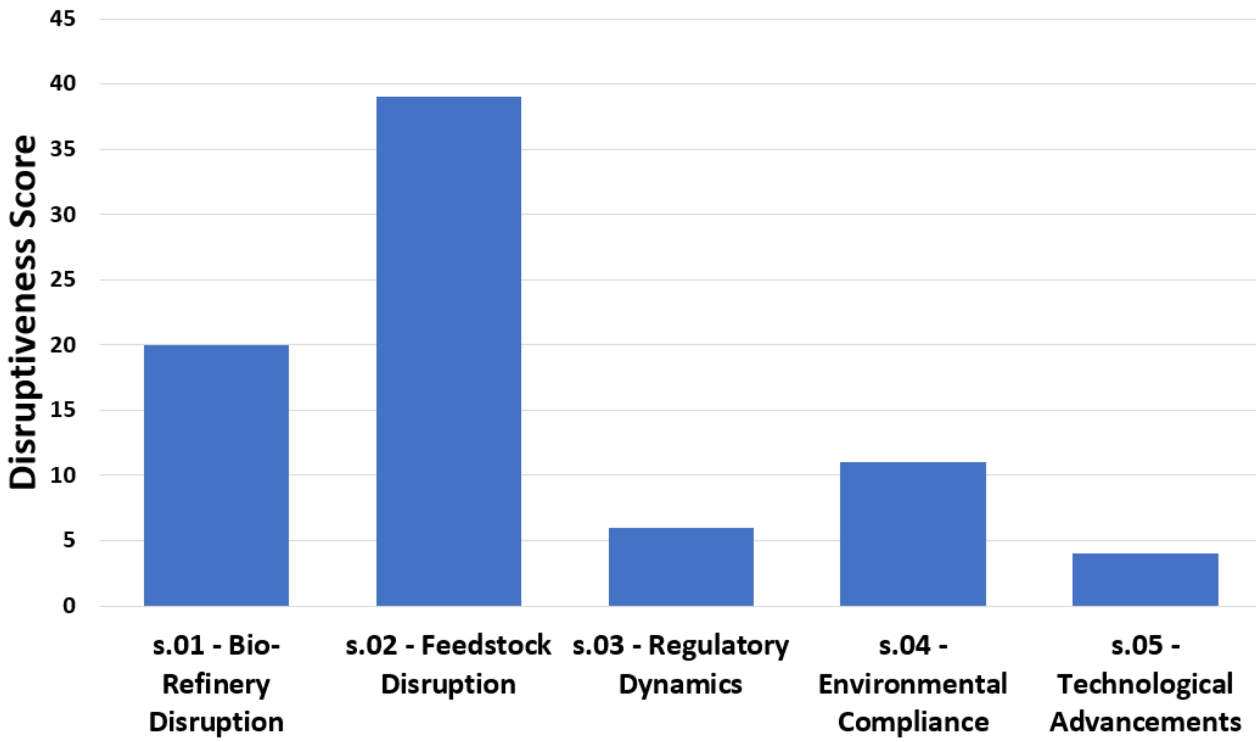



**FIGURE 30. The disruptiveness score of scenarios is based on the sum of squared differences in the priority of initiatives relative to the baseline scenario for the SAF supply chain system development. These are the critical scenarios where the risk and safety factors may be disrupted.**

This section describes how various scenarios impact the system's order and examines the role of the logical and functional architecture in shaping priority decisions. Figure 30 presents the disruptiveness scores for each scenario, with values normalized to a maximum of 100. Notably, three scenarios—*s.03* (*Regulatory Dynamics*), *s.04* (*Environmental Compliance*), and *s.05 (Technological Disruptions*)—register relatively low disruptiveness scores, ranging from four to twelve, indicating minor levels of disruption on the normalized scale. This suggests that these scenarios do not substantially alter the functional activities related to the Supply Chain for Sustainable Aviation Fuel (SAF). Conversely, scenarios *s.01 - Bio-Refinery* and *s.02 Feedstock*

*Disruption* show significantly higher disruptiveness, indicating their potential to markedly reorder system initiatives within the architecture.

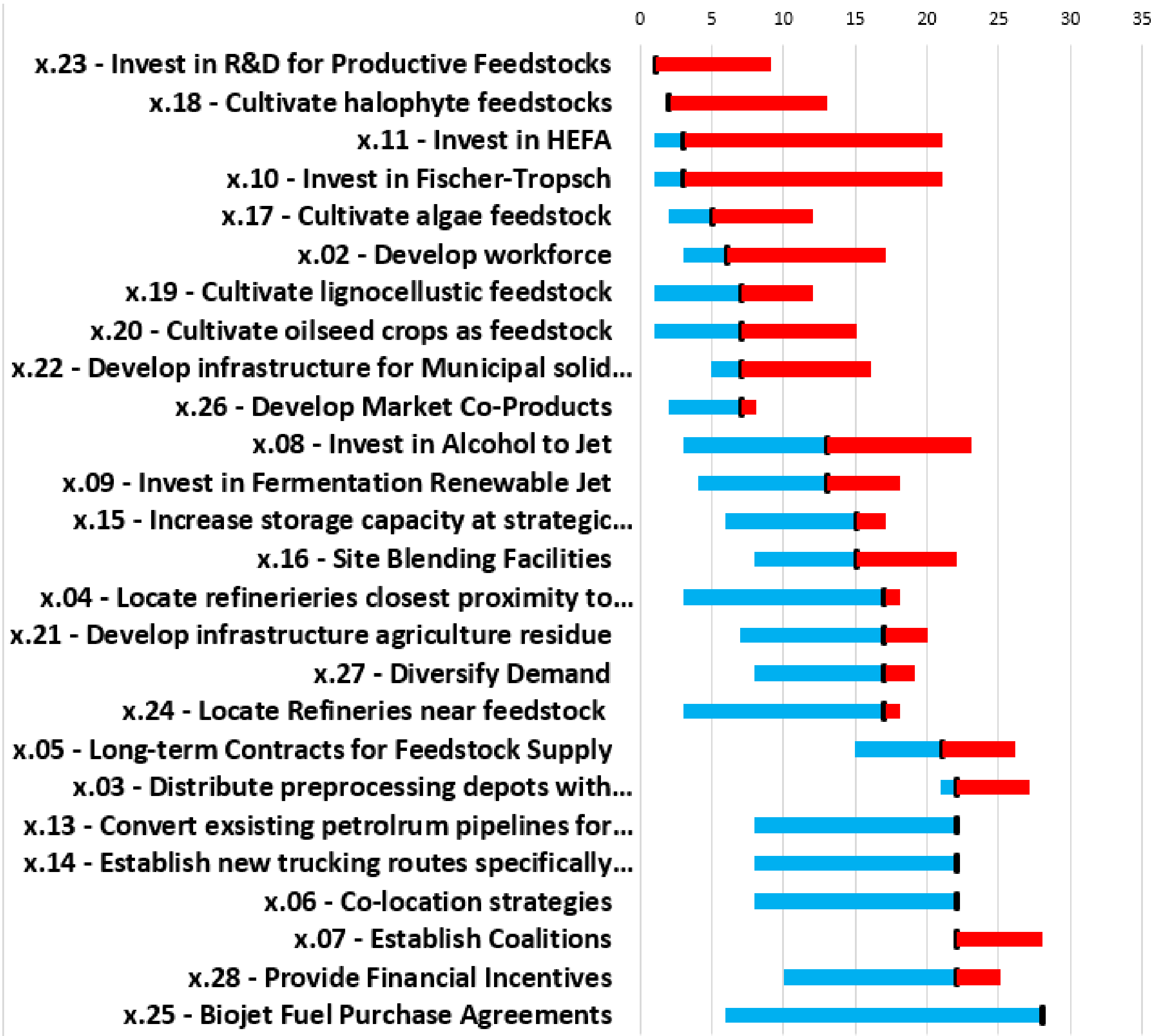



**FIGURE 31. Distributions of initiatives influence rankings based on which risk and safety factors could arise more often or do not occur for the Supply Chain for SAF. Blue indicates a promotion, and red indicates a demotion ranking.**

Figure 31 illustrates the findings from a case study that examines the baseline ordering of twenty-eight initiatives by a system's functional and logical architecture. The initiatives are ranked for both the baseline and various disruptive scenarios. In this figure, the black bar denotes the baseline ranking of each initiative (ranging from one to twenty-seven). The blue bar indicates the highest rank an initiative achieves under a disruptive scenario, and the red bar shows the lowest rank an initiative holds under such conditions. This visualization demonstrates the variability in initiative prioritization across different scenarios within the system development.

The most resilient initiatives are either highly ranked in both the baseline and under disruptive scenarios or may start with a lower baseline rank but ascend in importance when disrupted. For instance, initiative x.23 - Invest in R&D for Productive Feedstock, achieves the highest rank in a scenario where x.18 - Cultivate Halophyte Feedstock is prominent. Notably, five of the top ten initiatives are related to feedstock cultivation, aligning with specific functional and logical architecture areas. Conversely, the less resilient initiatives are ranked low in baseline and disruptive scenarios. An example is *x.25 – Bio-Jet Fuel Purchase Agreements*, which starts at a baseline of twenty-eight but can ascend to as high as 6th in some scenarios. However, the lowest seven initiatives are generally associated with later functions of the functional architecture, typically involving market development activities in the SAF supply chain.

The middle section of the figure shows initiatives that experience significant fluctuations in priority, making their ranking the most challenging to stabilize. These initiatives are primarily associated with infrastructure development and biorefinery technology phases of the SAF supply chain development.

## *5.4. Summary*

This chapter has described a multi-criteria impact analysis integrated with SysML to identify risk and safety factors through the system development of an SAF supply chain. The chapter described a framework for understanding disruptions in the system development of a supply chain for SAF. It describes the transition to SAF, driven by environmental goals and supported by various government initiatives. The study describes the necessity of integrating risk and safety factors into the SysML development life cycle for SAF supply chains. Using stakeholder input and existing literature, a custom SysML profile is developed to assess risks and safety, facilitating comprehensive Criteria-Initiative C-I and Criteria-Scenario C-S assessments. The analysis of scenarios reveals that Bio-Refinery and Feedstock Disruption scenarios have the highest disruptiveness, significantly affecting system priorities. In contrast, scenarios like Regulatory Dynamics, Environmental Compliance, and Technological Advancements show minimal disruption. This insight helps prioritize initiatives, especially those related to feedstock cultivation, which are crucial for the functional and logical architecture of the SAF supply chain.

# Chapter 6 | Synthesizing Best Practices and Advancement in Extending Risk Factors and Safety Factors in SysML

## *6.1. Introduction*

Chapter 6 describes the best practices and challenges for implementing risk and safety factors in the SysML model. The recommendations in this study are based on experience with implementing case studies. Section 6.2 describes the recommended uses of SysML. Section 6.3 identifies best practices for integrating risk and safety factors. Section 6.4 describes the lessons learned and challenges associated with applying the framework.

## *6.2. Identifying Best Practices for SysML*

This section describes best practices for integrating risk and safety factors in SysML. Section 6.2.1. Describes the best practice for establishing clear definitions and objectives for risk and safety factors. Section 6.2.2. describes establishing incremental and iterative development for integrating risk and safety factors. Section 6.2.3. describes the best practices for traceability between collaborators and how risk and safety factors are traced throughout the. Section 6.2.4. describes the importance of establishing a consistent and standard framework for integrating risk and safe factors into SysML. Section 6.2.5. refers to implications training and skill development for the SysML.

### 6.2.1 Early and Continuous Stakeholder Involvement

Engage stakeholders from the earliest stages of the project to ensure that their needs and concerns are thoroughly understood and addressed. Early involvement helps capture a comprehensive set of requirements and fosters stakeholder buy-in, which is crucial for successful project implementation. In the smart parking lot case study, stakeholders such as drivers, municipal corporations, and law enforcement agencies helped define clear system criteria and operational capabilities.

### 6.2.2. Comprehensive Requirement Elicitation

Utilize multiple techniques for requirement elicitation, including interviews, surveys, workshops, and literature reviews. A diverse set of techniques ensures that all relevant requirements are captured, reducing the risk of missing critical aspects. For example, the SAF supply chain project employed a combination of stakeholder interviews and literature reviews to gather comprehensive system requirements and criteria.

## 6.3. Best Practices for Integrating Risk and Safety

### *6.3.1. Clear Definition and Objectives for Risk and Safety Factors*

This dissertation defines risk and safety factors; it is important to note that they can appear ambiguously across various systems and architectures. Therefore, it is crucial to establish the context in which a risk manager identifies risk and safety factors. Additionally, defining the objective early in system development is essential to capture the risk and safety factors that align with system goals. For example, when applying MCIA within the framework for the system development of a smart parking lot system, a system architecture establishes the concept operations and system requirements. The case then leverages the CONOPS and system requirements to create risk and safety factors. For example, stakeholders in law enforcement can survey the smart parking lot system to secure the premises and track suspect vehicles; therefore, we can trace those capabilities to risk and safety factors. i.e., es. *Police Presence* & er. *Vehicle Theft.* This best practice allows users to understand how risk and safety are generated and traced based on the systems engineering lifecycle and enables unambiguity for stakeholders involved.

### *6.3.2. Incremental and Iterative Development for Integrating Risk and Safety*

The study utilized a comprehensive framework to integrate risk and safety factors across various applications. With the advancement of this framework, engineers, risk managers, and many more will be able to visualize the interactions within a system. Therefore, iterative updates are performed by identifying new stakeholders, risk and safety factors, and system requirements based on the impact of system disruptions on activities within the functional architecture.

### *6.3.3. Consistency and Standardization*

There is a need to establish consistency and standards within the system's framework. Previous studies have employed ISO to build security and safety management frameworks in SysML. Consistency ensures that all diagrams are displayed without fluctuation or variation when applying risk factors. Consistency leads to unambiguous communication amongst stakeholders. For example, the custom stereotype adapted from the MCIA standard was applied to various activities within the functional architecture and is used similarly to make applying risk and safety consistent. Adding this stereotype is advantageous because it enables the creations to account for risk and controls usually included in their original format stakeholders to evaluate criteria and functions quantitatively to assess the impact.

### *6.3.4. Custom SysML Profiles for Risk-Safety Integration*

Another best practice is to develop custom SysML profiles that explicitly incorporate risk and safety factors into the system model. The purpose of developing custom SysML profiles is to assist in facilitating the visualization and analysis of risks and safety measures within the system architecture, making it easier to identify and mitigate potential hazards. For example, the smart parking lot system used a custom SysML profile to integrate risk-safety factors into the functional and logical architecture, helping to identify vulnerabilities and implement safety measures.

### *6.3.5. Development of Criteria and Scenarios*

Another best practice is defining success criteria and developing scenarios to evaluate system performance under different conditions. Implementing these practices aims to help prioritize understanding how different factors influence system performance and prioritize initiatives based on their impact. For example, the smart parking lot and SAF supply chain case study. Another best practice is intertwining the MCIA results with SysML models to represent how different scenarios visually impact the system.

## *6.4. Lesson Learned Risk and Safety Factors*

The section describes the challenges of integrating risk and safety factors in SysML. Section 6.3.1. describes learning curve challenges for using SysML. Section 6.3.2 describes the challenges associated with integrating risk and safety in existing processes on the job. Section 6.3.3 describes the challenges for establishing clarity for users in SysML. Section 6.3.4 specifies the challenges of selecting tools for integrating risk and safety factors.

### *6.4.1. Learning Curve*

Although SysML is a powerful modeling language, it presents a challenge when implementing supporting aspects, such as risk and safety factors, due to the system modeling language's steep learning curve. According to (Shevchenko, 2020), system architects should create models that represent the system with sufficient simplicity to clarify its structure and behavior while managing complexity. Architects must ensure that the models accurately reflect the system, and conversely, the system should validate the model. To enhance the model's capability to monitor risk and safety, architects must consider factors related to architecture, risk, and safety. This requirement is underscored by various case studies that illustrate different systems and how risk and safety interact within dynamic environments. Architecture-related risks—including technological, integration, and operational risks—can significantly affect the system’s ability to meet its objectives. Therefore, when integrating risk and safety measures into the architecture, it is advisable to iteratively identify emergent conditions and develop applicable scenarios for the system model.

### *6.4.2. Integrating Risk and Safety*

Using SysML for modeling risk presents several advantages, including supplementary visualization, traceability, and integration with system architecture. However, there are notable disadvantages and challenges associated with this approach. Effective use of SysML for risk modeling necessitates that risk managers possess both the necessary toolset and proficiency in SysML. This includes understanding SysML diagrams, profiles, and stereotypes. A significant learning curve is associated with acquiring these skills, potentially requiring dedicated training and ongoing support for risk managers. Suppose the SysML model is limited to capturing only functional architecture-related risk and safety factors. In that case, it may overlook broader program risks critical to comprehensive risk management. This scope limitation can lead to risk and safety data duplication across different tools and models, as broader risks must be managed outside the SysML environment. This duplication can result in inconsistencies and increased effort in maintaining and synchronizing data. Managing risks that extend beyond the system architecture may require multiple tools, leading to a fragmented risk management process. This fragmentation complicates the consolidation and analysis of risk data, reducing the efficiency and effectiveness of the risk management process. Integrating risk data from various tools into a cohesive risk management strategy can be challenging, particularly when ensuring consistency and traceability across different platforms. Incorporating all program risks into the SysML model can include risks without direct traceability to the system architecture. These non-architectural risks, such as market or regulatory risks, do not have precise relationships with system components, leading to a lack of actionable links within the SysML model. Including these unrelated risks can clutter the SysML model, making it more complex and challenging to manage. This can detract from the primary focus of SysML, which is to model the system’s architecture and behavior.

### *6.4.3. Application of MCIA*

One of the major challenges when implementing the MCIA to the SysML as a singular framework to assess risk and safety for complex systems is processing the information into a spreadsheet. The goal is to load MCIA inputs from SysML to a spreadsheet automatically so disruptive scenarios and initiatives are quantitatively measured and ranked for corresponding activities within the system lifecycle. To begin with, XMI file code is written in a hierarchical format, which makes it inherently complex to understand when first viewing where SysML models are stored. In addition, the SysML model consists of various diagram types such as requirements, activity, and block definition diagrams; therefore, there is a need to interpret how to distinguish and precisely select when extracting information from any SysML diagrams. Furthermore, the use of stereotypes in SysML (custom diagrams) for storing risk and safety information is challenging to extract because they are nested elements, relationships, and attributes that need to be parsed and converted into proper data type and without thew knowing to execute this it can be very tedious and error prone. To properly automate the process and ultimately minimize error, the framework user should check for consistency in naming convention so that data representative of all models is shown within SysML.

```
▼<xmi:XMI xmlns:xmi="http://schema.omg.org/spec/XMI/2.1" xmlns:uml="http://schema.omg.org/spec/UML/2.1"
 xmlns:SysML="http://www.omg.org/spec/SysML/20161101/SysML" xmi:version="2.1">
  <xmi:Documentation exporter="Enterprise Architect" exporterVersion="6.5" exporterID="1628"/>
 ▼<uml:Model xmi:type="uml:Model" name="EA_Model" visibility="public">
  ▼<packagedElement xmi:type="uml:Package" xmi:id="EAPK_7C0772E0_7AE9_41d1_907D_FECC23889B89" name="Activity Pkg"
   visibility="public">
     <packagedElement xmi:type="uml:Class" xmi:id="EAID_3AFB20C6_73FB_4acc_9289_2942B9376262" name="Agriculture Residue"
     visibility="public"/>
     <packagedElement xmi:type="uml:Dependency" xmi:id="EAID_4E121FEC_B9A1_4472_B058_688A7659D18E" visibility="public"
     supplier="EAID_D610794B_E0C5_4cb3_90C3_7CC306F6BD71" client="EAID_3AFB20C6_73FB_4acc_9289_2942B9376262"/>
     <packagedElement xmi:type="uml:Class" xmi:id="EAID_7E69D18F_4281_4484_82A5_4867514F952F" name="Alchol to Jet"
     visibility="public"/>
     <packagedElement xmi:type="uml:Dependency" xmi:id="EAID_6B4E2420_D415_41e2_95D3_A55AEAFA3D84" visibility="public"
     supplier="EAID_478B5005_B948_4e11_9F5C_526E6C14801F" client="EAID_7E69D18F_4281_4484_82A5_4867514F952F"/>
    ▼<packagedElement xmi:type="uml:Class" xmi:id="EAID_32F95A33_CA98_411d_8EEE_A99A7530087D" name="Algae"
     visibility="public">
       <generalization xmi:type="uml:Generalization" xmi:id="EAID_4EA8F84C_8727_4779_BB8A_A0A7F2F325BC"
       general="EAID_45E63C31_12D9_4fc6_9DA6_E17FD061BB47" isSubstitutable="true"/>
     </packagedElement>
    ▼<packagedElement xmi:type="uml:Class" xmi:id="EAID_478B5005_B948_4e11_9F5C_526E6C14801F" name="Bio-Refining
     Technologies" visibility="public">
      ▼<ownedAttribute xmi:type="uml:Property" xmi:id="EAID_dst7770D4_0C3E_431b_B4A1_A9BCA11BA0BA" visibility="public"
       association="EAID_7C7770D4_0C3E_431b_B4A1_A9BCA11BA0BA" isStatic="false" isReadOnly="false" isDerived="false"
       isOrdered="false" isUnique="true" isDerivedUnion="false" aggregation="none">
         <type xmi:idref="EAID_9A4CDAC8_6B64_4e76_9F8F_905AFFE28CF8"/>
       </ownedAttribute>
      ▼<ownedAttribute xmi:type="uml:Property" xmi:id="EAID_2EA1B1E5_970E_42c3_AD35_0A23ED3F9D94" visibility="public"
       aggregation="composite" isStatic="false" isReadOnly="false" isDerived="false" isOrdered="false" isUnique="true"
       isDerivedUnion="false">
         <type xmi:idref="EAID_45E63C31_12D9_4fc6_9DA6_E17FD061BB47"/>
       </ownedAttribute>
     </packagedElement>
    ▼<packagedElement xmi:type="uml:Association" xmi:id="EAID_7C7770D4_0C3E_431b_B4A1_A9BCA11BA0BA" visibility="public">
       <memberEnd xmi:idref="EAID_dst7770D4_0C3E_431b_B4A1_A9BCA11BA0BA"/>
       <memberEnd xmi:idref="EAID_src7770D4_0C3E_431b_B4A1_A9BCA11BA0BA"/>
      ▼<ownedEnd xmi:type="uml:Property" xmi:id="EAID_src7770D4_0C3E_431b_B4A1_A9BCA11BA0BA" visibility="public"
       association="EAID_7C7770D4_0C3E_431b_B4A1_A9BCA11BA0BA" isStatic="false" isReadOnly="false" isDerived="false"
       isOrdered="false" isUnique="true" isDerivedUnion="false" aggregation="composite">
         <type xmi:idref="EAID_478B5005_B948_4e11_9F5C_526E6C14801F"/>
       </ownedEnd>
     </packagedElement>
     <packagedElement xmi:type="uml:Class" xmi:id="EAID_EAA4B685_D86D_495d_91DE_A237AD3A47FE" name="City Metropolitan
     Areas" visibility="public"/>
     <packagedElement xmi:type="uml:Dependency" xmi:id="EAID_0A431EEB_9F63_4c14_A006_88B74E318EA3" visibility="public"
     supplier="EAID_C0A3F1DB_127D_48f6_B5B8_B72DE9D93288" client="EAID_EAA4B685_D86D_495d_91DE_A237AD3A47FE"/>
    ▼<packagedElement xmi:type="uml:Class" xmi:id="EAID_45E63C31_12D9_4fc6_9DA6_E17FD061BB47" name="Feedstock"
     visibility="public">
      ▼<ownedAttribute xmi:type="uml:Property" xmi:id="EAID_dst281D0A_0518_402d_A16B_67C4062674F9" visibility="public"
       association="EAID_71281D0A_0518_402d_A16B_67C4062674F9" isStatic="false" isReadOnly="false" isDerived="false"
       isOrdered="false" isUnique="true" isDerivedUnion="false" aggregation="none">
         <type xmi:idref="EAID_9A4CDAC8_6B64_4e76_9F8F_905AFFE28CF8"/>
       </ownedAttribute>
      ▼<ownedAttribute xmi:type="uml:Property" xmi:id="EAID_5033058D_3EC8_463e_8AB8_7C7CABDF0243" visibility="public"
       aggregation="composite" isStatic="false" isReadOnly="false" isDerived="false" isOrdered="false" isUnique="true"
       isDerivedUnion="false">
         <type xmi:idref="EAID_9A4CDAC8_6B64_4e76_9F8F_905AFFE28CF8"/>
```


**FIGURE 32. Example of XMI file that stores Information related to SysML diagrams.**

## *6.5. Discussion*

This section will synthesize the best practices and challenges in implementing risk and safety factors within SysML models. Drawing from the case studies on the Smart Parking Lot System and SAF supply chain, we distill actionable insights and recommendations for effectively integrating these critical factors into SysML frameworks. Additionally, we highlight the essential steps and considerations for ensuring the consistent and comprehensive application of risk and safety assessments throughout the system development lifecycle.

Establishing clear definitions and objectives for risk and safety factors early in the system development process is paramount. This clarity ensures that all stakeholders mutually understand these factors and their importance. By aligning the risk and safety objectives with the overall system goals, you can better capture relevant factors and mitigate potential issues effectively. Adopting an incremental and iterative approach for integrating risk and safety factors allows for continuous improvement and adaptation to new challenges. This method ensures that risk assessments remain relevant as the system evolves, incorporating changes in stakeholder values, emerging technologies, and policy updates. Iterative development helps in minimizing errors and enhancing the robustness of the system. It is crucial to consistently apply risk and safety factors across all SysML diagrams. Establishing standard practices, such as using ISO frameworks for security and safety management, ensures that all stakeholders interpret and utilize the diagrams uniformly. Consistent application of custom stereotypes and standardized practices, as demonstrated in the case studies, leads to unambiguous communication and efficient risk management.

Maintaining traceability of risk and safety factors throughout the system development lifecycle is vital for effective risk management. This involves linking risk factors to specific system components and processes, ensuring that any changes in the system are reflected in the risk assessments. Effective traceability facilitates easier identification of risk sources and their impacts, promoting proactive risk mitigation. Ensuring that team members possess the necessary skills to utilize SysML effectively is essential. Providing comprehensive training and continuous professional development helps build proficiency in SysML tools and techniques. This investment in training enhances the team's overall capability to integrate and manage risk and safety factors efficiently. One of the significant challenges in implementing SysML with risk and safety factors is the steep learning curve. SysML requires a deep understanding of its various diagrams, profiles, and stereotypes. New users often need help with the complexity of creating accurate and meaningful models. Overcoming this challenge necessitates targeted training programs and practical experience through iterative application.

Integrating risk and safety factors with existing processes can be challenging. Many organizations have established procedures and tools for risk management that may need to align with SysML. This misalignment can lead to redundancy and consistency, necessitating a careful approach to integrate SysML without disrupting existing workflows. Ensuring all users understand SysML models and the integrated risk and safety factors can be difficult. Ambiguities in the model can lead to misinterpretations and ineffective risk management. Developing comprehensive documentation and standardized practices helps establish clarity and consistency.

Selecting the appropriate tools for integrating risk and safety factors with SysML models. The chosen tools must support the required functionalities and facilitate seamless integration with other systems and processes. Ensuring compatibility and ease of use can help overcome the fragmentation of risk management processes and improve overall efficiency.

## *6.6. Summary*

Chapter 6 describes the best practices and challenges of integrating risk and safety factors into SysML models. Cases are leveraged to establish such practices that evoke clear definitions and objectives. Case studies provide context to fulfill processes such as incremental and iterative development, consistency maintaining traceability, and research and development.

However, challenges like the steep learning curve, integration with existing processes, establishing clarity, and selecting appropriate tools were highlighted. Addressing these challenges requires a strategic approach that involves continuous learning, effective communication, and the reasonable selection of tools and methodologies.

By adhering to the recommendations detailed in this chapter, organizations can significantly bolster their ability to manage risks and ensure safety within complex systems. This, in turn, can lead to improved project success and reliability. The systematic approach enhances the ability to integrate risk and safety factors. It cultivates a culture of proactive risk management and continuous improvement.

# Chapter 7 | Comparative Analysis

## *7.1. Introduction*

This chapter provides an in-depth overview of the methodological approach used in this dissertation and includes a detailed comparison of state-of-the-art methods. This chapter establishes a clear comparison of relevant criteria. Section 7.2 compares the nature of the cases to see how one case needs real-time information while the other does not, establishing a clear, relevant criteria comparison. The criteria should align with key performance indicators that stakeholders are interested in. This chapter conducts an ablation study to determine the significance of removing components such as risk and safety factors to evaluate their impact independently.

## *7.2. Comparing Case Studies*

Despite both case studies focusing on high-impact logistic systems, they exhibit significant differences in human actor engagement. Real-time data is crucial for reservation and availability checks in the smart parking lot system, relying heavily on a central computing system to process these functions. This time-sensitive nature necessitates risk and safety factors that can respond quickly to emerging risks. Conversely, the sustainable aviation fuels (SAF) supply chain emphasizes long-term data and logistics planning, making it less dependent on real-time information. Consequently, the SAF supply chain's risk and safety factors are geared towards long-term strategic responses rather than immediate action. Therefore, it is essential to list and evaluate safety factors that can effectively address risks within the smart parking lot system, considering its unique real-time requirements.

Due to the long-term planning and system complexity, the outcome of system disruptions is not expected to impact the system immediately. However, it can cause latent errors that alter how stakeholders establish system requirements. On the other hand, the time sensitivity of the smart parking lot case causes the effect of the disruptions to be actively recognizable. On the other hand, the case related to the smart parking system will reveal how the function and system requirements actively impact disruptions. Therefore, the distinguishing factor between the cases studied is using the time constraints in the SysML model for activities within the functional architectures, placing bounds on the duration of critical functions.

Another distinguishing factor across the studies is the spatial context in which they operate and how the spatial resolution scale impacts the SysML model and the multi-criteria impact analysis. For instance, the root origin of the SAF supply chain is feedstock cultivation, which ends with the fueling of the jet. Its complexity in reaching various stakeholders with unique responsibilities makes it imperative to capture risk and safety factors associated with the phases of the supply chain. On the other hand, the smart parking lot system is confined within a zone, but there is still a supply of risk and safety factors. Instead, it means fewer unique influences on capturing risk and safety factors.

## *7.3. Comparative Analysis*

The study introduces a proposed methodology that theoretically integrates risk and safety factors within the Systems Modeling Language (SysML) framework. This approach aims to systematically identify, assess, and manage risk and safety throughout the system development lifecycle, utilizing SysML as the core modeling language. This integration creates a comprehensive model incorporating risk and safety factors into the system architecture. The study develops custom SysML stereotypes tailored to effectively capture and communicate risk and safety information to achieve accurate representation within the functional architecture.

To evaluate the effectiveness of the proposed methodology, a comparative analysis was conducted against benchmark methods currently recognized in the field. These state-of-the-art methods were identified through a thorough review of academic resources, including Google Scholar and IEEE Xplore. The comparison is based on several critical criteria essential for effectively integrating supporting aspects of risk and safety in Model-Based Systems Engineering (MBSE).

The following comparative analysis indicates four criteria most desirable for integrating supporting aspects of risk and safety in MBSE. *Modeling Language and Tools* refers to mapping the semantics of a system specification from a natural language to an abstract, facilitating easier understanding and compact representation of complex systems (McGregor & Cohen, 2022). *Integration of Risk Management* refers to the extent to which a methodological approach incorporates risk management. *Integration of Safety Management* refers to the extent to which a methodological approach incorporates safety management. *Usability and Adaptability* refer to how user-friendly and efficient the methods are in practice, while adaptability denotes their flexibility and ability to customize for various applications and contexts. *Effectiveness* is measured by the application in which these methods have been used.

**TABLE 32. Comparative Analysis of Proposed Method and Benchmark Methods**

| Methods | Proposed Method | UML | BPRIF | STPA | FMEA |
|---|---|---|---|---|---|
| Modeling Language and Tools | SysML | UML | adoBPRIM | STPA | N/A |
| Integration of Risk Management | Comprehensive | Limited | Extensive | Extensive | Extensive |
| Integration of Safety Management | Comprehensive | None | Limited | Extensive | Limited |
| Usability and Adaptability | High | Medium | Medium | High | Medium |
| Effectiveness | Proven in SAF and Smart Parking Lot | Proven in software systems | Proven in business processes | Proven in safety-critical system | Proven in various industries |

Table 32 is a comparative analysis designed to describe the pros and cons of various methodologies in the context of risk and safety management modeling. This table will assist decision-makers in various industries in choosing a methodological approach to significantly improve project outcomes according to the criteria within this table.

## *7.4. Ablation Study*

The section conducts an ablation study to assess the importance of various elements in the Multi-Criteria Impact Analysis. The study is performed on the SAF supply chain system development case for the methodological approach's components. An ablation study systemically removes or alters the components of the methodological approach to understand their overall impact on system performance.

The following equation was used to test the impact of component ablations on overall system performance. In this case, the accuracy metrics indicate the correctly ranked component compared to the baseline ranking. Equation (6) measures the accuracy of the matching ranks for the initiatives.

$$Accuracy = \frac{\#\ of\ Matching\ Ranks}{Total\ \#\ of\ Ranks} * 100 \tag{6}$$

For example, if twenty-eight out of seven ranks match the baseline proposed approach, The accuracy would be 7/28 * 100, equivalent to 25%. On the other hand, Equations 7-8 determine the deviation between the higher and lowest rankings through ablation. The deviation measures the mean difference.

$$d_i = d_{baseline} - d_{ablates} \tag{7}$$

$$Deviation = \frac{\Sigma_{i=1}^{\mathrm{n}} |d_i|}{n} \tag{8}$$

In equation (7), n is the total number of ranks in the ablated and baseline ranking I regarded as the i-th initiative.

$$d^* = \frac{1}{n} \Sigma_{i=1}^{\mathrm{n}} |d_i| \tag{9}$$

The standard deviation of ($s_d$) I calculated as equation (10):

$$s_d = \sqrt{\left(\frac{1}{n-1}\right)} \Sigma_{\mathrm{i}=1}^{n} (d_i - d^*)^2 \tag{10}$$

$$t = \frac{d^*}{s_d/\sqrt{n}} * 100 \tag{11}$$

The t-test compares the means of two related groups to determine if there is a statistically significant difference between them. In this case, the equation evaluates whether the rank difference between the baseline and ablate scenarios is statistically significant. A higher t-statistic and low p-value (typically less than 0.05) suggests that the difference is significant and is not due to random chance.

Table 32 shows that integrating risk and safety factors as the baseline method significantly influences the ranking accuracy and deviation. The ablation study contributes to the findings by examining the impact of removing these factors on the overall results and how they deviate from the baseline contribution. The results suggest that ablating risk factors has a higher influence on the promotion and demotion of each initiative than safety factors. The deviation observed from the study indicates that removing risk factors causes a substantial deviation from the baseline rankings.

**TABLE 33. Ablation Study of Multi-Criteria Impact Analysis on SAF Supply Chain Case Study. Here, RF = Risk Factors Ablation and SF = Safety Factors Ablation show accuracy and deviation.**

| Components | Accuracy | Deviation |
|---|---|---|
| **SF High Ranking** | 14.29 % | 2.54 |
| **SF Low Ranking** | 17.86 % | 4.36 |
| **RF High Ranking** | 7.14 % | 4.64 |
| **RF Low Ranking** | 14.29 % | 5.43 |

**TABLE 34. Ablation Study of Multi-Criteria Impact Analysis on SAF Supply Chain Case Study. Here, RF = Risk Factors Ablation, and SF = Safety Factors Ablation, showing T-Statistic and p-value.**

| Components | T-Statistic | p-value |
|---|---|---|
| **SF High Ranking** | 4.46 | $7.95\ x\ 10^{-5}$ |
| **SF Low Ranking** | -3.48 | 0.00171 |
| **RF High Ranking** | 4.83 | $4.85\ x\ 10^{-5}$ |
| **RF Low Ranking** | -6.12 | $1.53\ x\ 10^{-6}$ |

In the case of the SAF supply chain, the ablated risk and safety factors are used to determine the T-statistic and p-value for the disruptions.

**TABLE 35. Ablation study for the disruptive scenarios calculating the t-statistic and p-value.**

| Components | T-Statistic | p-value |
|---|---|---|
| **SF** | 1.71 | 0.161489 |
| **RF** | 0.6015 | 0.579875 |

The high absolute t-statistic and low p-value for the ablation comparisons of low- and high-ranking risk factors indicate significant ranking changes. This demonstrates the critical importance of including risk factors in the assessment, as their removal leads to substantial changes in the promotion and demotion of initiatives. These results highlight how crucial risk factors are in determining the impact of an initiative within the SAF supply chain's functional architecture. Excluding these factors can result in significant deviations from the baseline, potentially overlooking key risks and mechanisms essential for understanding system performance.

Including safety and risk factors ensures that potential hazards and uncertainties are adequately considered, leading to more accurate and reliable rankings. The ablation study shows that both factors are necessary for capturing the true impact of initiatives. Without them, the rankings can be misleading, emphasizing the need for comprehensive multi-criteria impact analysis models that integrate various factors.

The findings from Tables 32 and 33 emphasize the need for incorporating risk and safety factors in multi-criteria impact analyses. The significant deviations observed when these factors are removed underscore their importance in maintaining accurate and reliable rankings. By ensuring these factors are included, decision-makers can make more informed choices, optimize resource allocation, and enhance the sustainability and effectiveness of the SAF supply chain.

According to Table 34's statistical analysis results, there are no statistically significant changes in the rankings of initiatives within the SAF supply chain because of the ablation of safety factors (SF) and risk factors (RF). Since the p-values for SF and RF are larger than 0.05, it is more likely that random variation than eliminating these factors is to blame for the observed differences. These results imply that the model's rankings are largely stable and do not rely significantly on including safety and risk factors; however, more research uses different datasets and scenarios.

In this study, the dissertation performs an ablation study; we evaluate the impact of integrating SysML into developing the (SAF) supply chain model. The dissertation compares the model's performance with and without SysML by examining initiative rankings across various scenarios.

**TABLE 36. Ablation study of MCIA on SAF case. This case removes the modeling language as a study component and analyzes how the MCIA performs independently when ranking scenarios against initiatives.**

| Scenario | Mean Difference | Std Dev of Differences | RMSE |
|---|---|---|---|
| ***s.01*** | 3.36 | 12.55 | 11.51 |
| ***s.02*** | 0.43 | 12.27 | 10.62 |
| ***s.03*** | 1.57 | 13.02 | 10.98 |
| ***s.04*** | 1.86 | 12.47 | 10.67 |
| ***s.05*** | -0.14 | 12.48 | 10.66 |

Table 36 provides a detailed comparison of scenarios when a modeling language is utilized versus when it is absent. The results demonstrate that a modeling language significantly influences the ranking of scenarios among initiatives. Using graphical representations in the functional architecture is crucial, as it effectively illustrates the direct relationships between one initiative and the next. Consequently, integrating risk and safety factors with the MCIA within the SysML framework proves to be highly beneficial for decision-makers. This integration enhances the clarity and effectiveness of decision-making processes by providing a structured and visual approach to understanding complex interactions within the system.

The result across scenarios indicates that the impact varies depending on the analysis of the system with and without the modeling language. For instance, scenarios s.01, s.03, and s.04 indicate that adding the modeling language positively impacts ranking effectiveness. On the other hand, scenarios s.02 and s.05 have medium to low impact, respectively, meaning that the modeling language didn't have much of a disruptive effect on scoring scenarios among initiatives.

The variation in impact as demonstrated by the standard deviations suggests that while the modeling language generally aids in system architecture and decision-making processes, its effectiveness can depend heavily on each scenario's specific characteristics or demands. The relatively consistent RMSE values across the scenarios suggest that the deviations from the model's predictions are moderately stable, which points to the model's reliability in various settings, albeit with differing levels of impact.

## *7.5. Summary*

Chapter 7 describes an overview of the methodological approach and a detailed comparison of state-of-the-art related to integrating risk and safety in MBSE. The chapter describes the differences between the case studies and how future case studies with similar attributes will have to capture risk. An ablation study is also conducted to assess the individual impacts of removing components like risk and safety factors, providing insights into their essential roles in system evaluation. The chapter concludes with a comparative analysis of the proposed methodology against benchmark methods. It uses SysML to enhance risk and safety management integration into system development, proving its effectiveness in various real-world applications.

# Chapter 8 | Conclusion

## *8.1. Introduction*

The chapter includes a description of the contributions, a summary of the conclusion, a dissertation schedule, and a timeline.

## *8.2. Summary of Contributions*

The contribution of the dissertation is characterized as follows:

**Contribution 1. Integration of risk and safety in MBSE characterizes the gap in integrating risk and safety into MBSE.**

This dissertation develops a novel framework that seamlessly integrates risk management and safety analysis within the MBSE process using SysML. Unlike existing methodologies that often treat these factors separately, this framework provides a unified approach to address both risk and safety factors.

**Contribution 2: Development and application of extended SysML stereotypes**:

The research extends SysML stereotypes to encapsulate both risk and safety factors, enhancing the ability to track and manage these factors within system models. This extension supports better traceability and communication of risk and safety information among stakeholders, improving the overall effectiveness of risk and safety management in complex engineering systems.

**Contribution 3. Implementation of multi-criteria impact analysis (MCIA) within SysML:**

The dissertation introduces the use of multi-criteria impact analysis to evaluate and prioritize system functions based on their impact under various disruptive scenarios. By integrating MCIA with SysML, the study provides a systematic method for assessing the importance of different criteria and initiatives, facilitating more informed decision-making.

**Contribution 4. Creation of a risk-safety profile within SysML**:

This work is an addition to the traditional risk management approach by integrating risk and safety factors into a single profile, represented as scenarios in SysML. This unified profile allows for a holistic assessment of how risk and safety factors interact and affect system performance, offering a more comprehensive view of potential impacts.

**Contribution 5. Empirical validation through several case studies:**

The proposed framework is validated through practical applications in two distinct case studies: a Smart Parking Lot System and the supply chain for Sustainable Aviation Fuels (SAF). These case studies demonstrate the adaptability and effectiveness of the framework across different engineering domains, showcasing its potential for widespread application.

**Contribution 6. Stakeholder communication and traceability**:

By integrating risk and safety factors within SysML, the dissertation significantly improves communication and traceability among stakeholders. This approach ensures that risk sources and controls are transparently documented and easily accessible, facilitating proactive risk mitigation and informed decision-making.

**Contribution 7. Theoretical framework for risk management in SysML**:

The dissertation contributes to the theoretical development of risk management frameworks by providing a detailed methodology for integrating risk and safety within SysML. This theoretical advancement offers a new perspective on managing risks in complex systems, addressing gaps in existing literature.

## *8.3. Summary of Conclusions*

This section summarizes the conclusions of the chapters above. The dissertation focuses on developing a novel framework that integrates risk and safety management into the model-based systems engineering (MBSE) process using SysML, enhancing the theoretical and practical aspects of risk management in complex systems.

## *8.4. Schedule and Timeline*

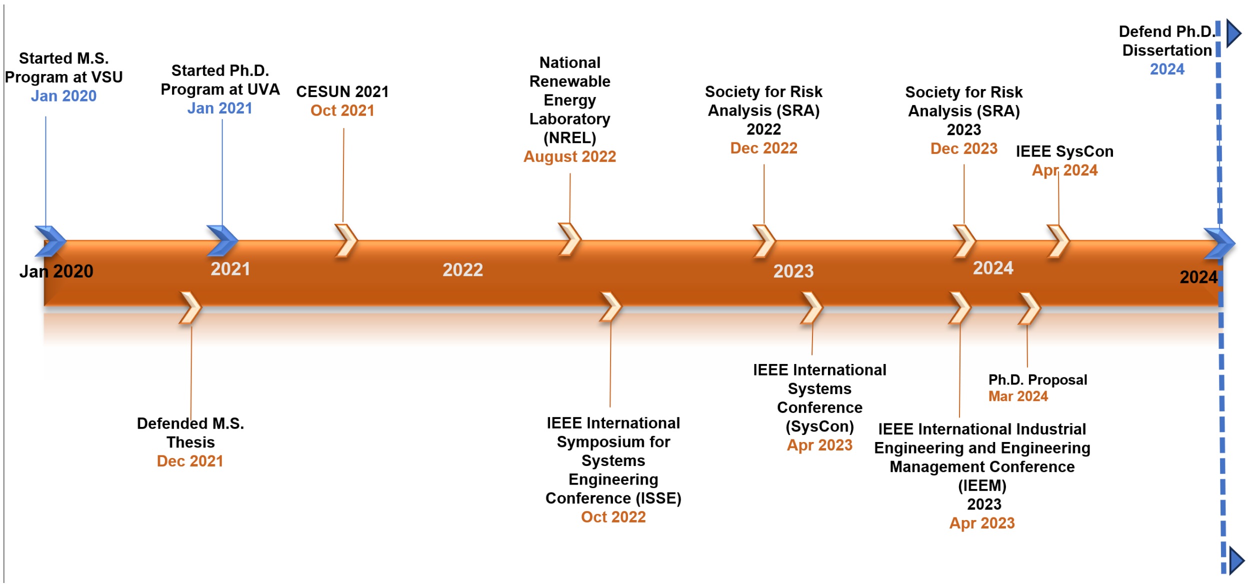



**FIGURE 33. Timeline of conference presentations and publications. Annotations above the timeline represent conference presentations, and annotations below the timeline show journal and conference publications.**

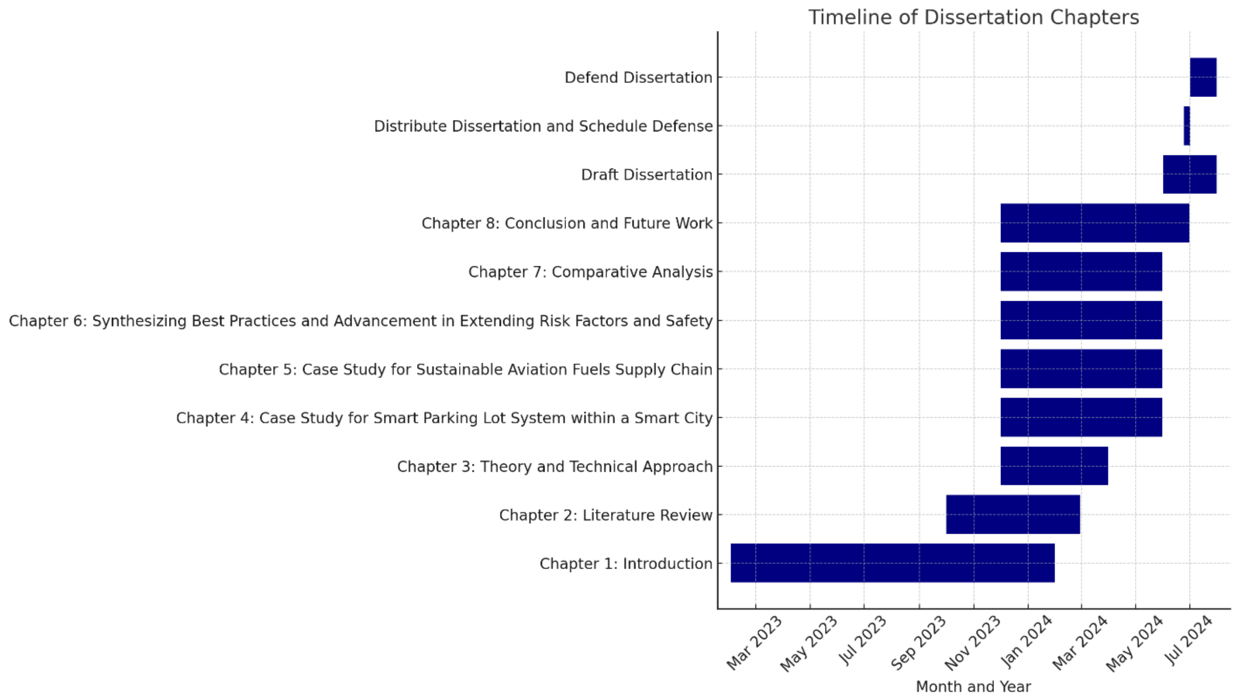



**FIGURE 34. Schedule of dissertation milestones.**

## *8.5. Summary*

Chapter 8 describes an overview of the research; this chapter describes the integration of risk and safety management within the MBSE process using SysML. The dissertation describes a novel framework that integrates risk management and safety analysis and extends SysML stereotypes to capture the factor implementing MCIA within SysML to evaluate and prioritize system functions under various scenarios. This study also describes the risk-safety profile for a holistic assessment, validated through case studies for the system development for the Smart Parking Lot System and SAF supply chain, demonstrating the framework's continuous evolution across multiple studies.

# References

Adedjouma, M., Thomas, T., Mraidha, C., Gerard, S., & Zeller, G. (2016). From document-based to model-based system and software engineering. Proceedings of the OSS4MDE.

Adekitan, A. I. (2018). Safeguards: A key process safety tool in jet fuel management from refinery to aircraft wings. *Process safety progress*, *37*(4), 518-524.

Ahlbrecht, A., & Durak, U. (2021, October). Integrating safety into MBSE processes with formal methods. In 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC) (pp. 1-9). IEEE.

Ajchariyavanich, C., Limpisthira, T., Chanjarasvichai, N., Jareonwatanan, T., Phongphanpanya, W., Wareechuensuk, S., ... & Pipattanasomporn, M. (2019, October). Park king: an IoT-based smart parking system. In *2019 IEEE International Smart Cities Conference (ISC2)* (pp. 729-734). IEEE.

Almutairi, A., Thorisson, H., Wheeler, J.P., Slutzky, D.L., & Lambert, J.H. (2018). Scenario-based preferences in development of advanced mobile grid services and a bidirectional charger network. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering, 4(04018017). https://doi.org/10.1061/AJRUA6.0000962

Airport Council International. (2022). A new study has been launched on the integration of sustainable aviation fuels at airports.

Aven, T., Ben-Haim, Y., Boje Andersen, H., Cox, T., Droguett, E. L., Greenberg, M., ... & Thompson, K. M. (2018, August). Society for Risk Analysis Glossary. In Society for Risk Analysis (pp. 3-9).

Aydin, I., Karakose, M., & Karakose, E. (2017, April). A navigation and reservation based smart parking platform using genetic optimization for smart cities. In *2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG)* (pp. 120-124). IEEE.

Bahill, A. T., Madni, A. M., Bahill, A. T., & Madni, A. M. (2017). Discovering system requirements. *Tradeoff Decisions in System Design*, 373-457.

Baker, R. M., Polmateer, T. L., Marcellin, M. C., Chen, T. D., Riggs, R. J., Iqbal, T., ... & Lambert, J. H. (2023, December). Mixed-Integer Programming with Enterprise Risk Analysis for Vehicle Electrification at Maritime Container Ports. In *2023 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1759-1766). IEEE.

Baklouti, A., Nguyen, N., Mhenni, F., Choley, J. Y., & Mlika, A. (2019). Improved safety analysis integration in a systems engineering approach. Applied Sciences, 9(6), 1246.

Baranwal, Gaurav, Dinesh Kumar, and Deo Prakash Vidyarthi. "A multi-criteria framework for smart parking recommender system." *2020 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2020.

Barriga, J. J., Sulca, J., León, J. L., Ulloa, A., Portero, D., Andrade, R., & Yoo, S. G. (2019). Smart parking: A literature review from the technological perspective. *Applied Sciences*, *9*(21), 4569.

Biggs, G., Post, K., Armonas, A., Yakymets, N., Juknevicius, T., & Berres, A. (2019, July). OMG standard for integrating safety and reliability analysis into MBSE: Concepts and applications. In INCOSE International Symposium (Vol. 29, No. 1, pp. 159-173).

Biggs, G., Juknevicius, T., Armonas, A., & Post, K. (2018, July). Integrating Safety and Reliability Analysis into MBSE: overview of the new proposed OMG standard. In INCOSE International Symposium (Vol. 28, No. 1, pp. 1322-1336).

Biyik, C., Allam, Z., Pieri, G., Moroni, D., O'fraifer, M., O'connell, E., ... & Khalid, M. (2021). Smart parking systems: Reviewing the literature, architecture and ways forward. *Smart Cities*, *4*(2), 623-642.

Buede, D. M., & Miller, W. D. (2024). The engineering design of systems: models and methods. John Wiley & Sons.

Carroll, E. R., & Malins, R. J. (2016). Systematic Literature Review: How is Model-Based Systems Engineering Justified?.

Chasson, H (2022). Integrating Safety Analysis in an MBSE Process

Chiaramonti, D. (2019). Sustainable aviation fuels: the challenge of decarbonization. Energy Procedia, 158, 1202-1207.

Clegg, K., Li, M., Stamp, D., Grigg, A., & McDermid, J. (2019). Integrating existing safety analyses into sysml. In Model-Based Safety and Assessment: 6th International Symposium, IMBSA 2019, Thessaloniki, Greece, October 16–18, 2019, Proceedings 6 (pp. 63-77). Springer International Publishing.

Connelly, E. B., Colosi, L. M., Clarens, A. F., & Lambert, J. H. (2015). Risk analysis of biofuels industry for aviation with scenario-based expert elicitation. Systems Engineering, 18(2), 178-191.

de Souza, F. G. R., de Melo Bezerra, J., Hirata, C. M., de Saqui-Sannes, P., & Apvrille, L. (2020, August). Combining STPA with SysML modeling. In 2020 IEEE International Systems Conference (SysCon) (pp. 1-8). IEEE

Management As an Element of the Smart City Concept. *Humanities and Social Sciences*, *30*(4-part 2), 45-60.

Doliente, S. S., Narayan, A., Tapia, J. F. D., Samsatli, N. J., Zhao, Y., & Samsatli, S. (2020). Bio-aviation fuel: a comprehensive review and analysis of the supply chain components. *Frontiers in energy research*, *8*, 110.

Douglass, B. P. (2015). *Agile systems engineering*. Morgan Kaufmann.

Ericson, C. A. (2011). Concise encyclopedia of system safety: Definition of terms and concepts. John Wiley & Sons.

Ericson C.A. (2015). Hazard Analysis Techniques for Systems Safety. John Wiley & Sons. ISBN 978-1-118-94038-9

Federal Aviation Administration. (2021). Aviation Climate Action Plan. Federal Aviation Administration. https://www.faa.gov/sites/faa.gov/files/2021-11/Aviation_Climate_Action_Plan.pdf

Hadj-Mabrouk, H. (2017). Preliminary Hazard Analysis (PHA): New hybrid approach to railway risk analysis. *International Refereed Journal of Engineering and Science*, *6*(2), 51-58.

Harahap, A. A., & Khamidi, M. F. (2024, February). Operation failure of risk analysis on floating storage and offloading. In IOP Conference Series: Earth and Environmental Science (Vol. 1298, No. 1, p. 012031). IOP Publishing.

Haskins, C. INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities; Wiley: New York, NY, USA, 2006

Henderson, K., & Salado, A. (2021). Value and benefits of model-based systems engineering (MBSE): Evidence from the literature. *Systems Engineering*, *24*(1), 51-66.

Hovorushchenko, T., Pavlova, O., & Kostiuk, M. (2023). Method of Increasing the Security of Smart Parking System. Journal of Cyber Security and Mobility, 297-314.

Hutchison, N., Pyster, A., & Cloutier, R. (2023). Using the Systems Engineering Body of Knowledge (SEBoK). *Systems Engineering for the Digital Age: Practitioner Perspectives*, 789-803.

Iacobescu, C., Oltean, G., Florea, C., & Burtea, B. (2021). Unified interplanetary smart parking network for maximum end-user flexibility. *Sensors*, *22*(1), 221.

INCOSE. (2018). Guide to the Systems Engineering Body of Knowledge (SEBoK) (v 1.9.1).

INCOSE (2023) Guide to SysML Model of a "Smart Parking Lot" Reference Archiutecture

INCOSE. 2010. Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. Version 3.2.1. San Diego, CA, USA: International Council on Systems Engineering (INCOSE), INCOSE-TP-2003-002-03.2.1: 362.

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 1-22.

ISO/IEC/IEEE. 2010. Systems and Software Engineering - System and Software Engineering Vocabulary (SEVocab). Geneva, Switzerland: International Organization for Standardization

(ISO)/International Electrotechnical Commission (IEC)/ Institute of Electrical and Electronics Engineers (IEEE). ISO/IEC/IEEE 24765:2010.

ISO/IEC. 2007. *Systems and Software Engineering -- Recommended Practice for Architectural Description of Software-Intensive Systems*. Geneva, Switzerland: International Organization for Standards (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 42010:2007.

Johnson, D. A., Melo, V., & Lambert, J. H. (2022, October). Risk Identification with Entity Attributes Diagrams in Business Process Modeling. In *2022 IEEE International Symposium on Systems Engineering (ISSE)* (pp. 1-8). IEEE.

Johnson, D. A., Wheeler, R., & Lambert, J. H. (2023, April). Risk Description Augmenting a Business Process Model. In *2023 IEEE International Systems Conference (SysCon)* (pp. 1-7). IEEE.

Johnson, D.A., Wheeler, R.L., Marcellin, M.C., Moghadasi, N., Altman, R., Lambert, J.H. (2024). Integration of Risk Sources and Risk Controls to SysML Requirement Diagram with Application to Sustainable Aviation Fuels. In *2023 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* (pp. 1-7) IEEE.

Joshi, N., Mittal, M., Jayawant, Y., Salunkhe, P., & Hattarge, M. (2021, July). Applying Systems Engineering framework for architecting a Smart Parking System within a Smart City. In *INCOSE International Symposium* (Vol. 31, No. 1, pp. 16-30).

Jurewicz , B. (2023) Risk management as an integral element of model-based system engineering (MBSE) using case studies and examples. *Integrate 24*

Kaufmann, U., & Schuler, R. (2016). Systems Re-Engineering-ein Beitrag zur Integration von MBSE und PLM. *Schulze, S.-O.; Tschirner, C.; Kaffenberger, R*, 343-353.

Krasner J. (2015) How Product Development Organizations can Achieve Long Term Cost Savings Using Model-Based Systems Engineering (MBSE)

Krishnan, R., & Bhada, S. V. (2020). An integrated system design and safety framework for model-based safety analysis. *IEEE Access*, *8*, 146483-146497.

Krishnan, R., & Bhada, S. V. (2022). Integrated system design and safety framework for model-based safety assessment. IEEE Access, 10, 79311-79334.

Kunnen, S. G., Adamenko, D., Pluhnau, R., & Nagarajah, A. (2019, July). An Approach to integrate risk management in cross-structure SysML-models. In *Proceedings of the Design Society: International Conference on Engineering Design* (Vol. 1, No. 1, pp. 3571-3580). Cambridge University Press.

Lambert, J. H., Polmateer, T. L., Loose, D., Eddy, T. L., Moghadasi, N., Johnson, D., & Manasco, M. C. (2023). Industry Supply Chain Disruption Analysis for Crater Planning District Commission. Commonwealth Center for Advanced Logistics Systems. https://www. ccals. com/wp-content/uploads/2022/01/Report_Industry_Supply_Chain_Disruption_Analysis_Crater_PDC_final. pdf. Accessed, 6.

Lee, D.S., Fahey, D.W., Skowron, A., Allen, M.R., Burkhardt, U., Chen, Q., Doherty, S.J., Freeman, S., Forster, P.M., Fuglestvedt, J., et al. (2021). The contribution of global aviation to anthropogenic climate forcing for 2000 to 2018. Atmospheric Environment, 244, 117834. https://doi.org/10.1016/j.atmosenv.2020.117834

Leveson, N. (2004). A new accident model for engineering safer systems. Safety science, 42(4), 237-270.

Li, C., Yu, Y., Leckning, J., Xing, W., Fong, C. L., Grundy, J., ... & Obie, H. O. (2021, July). A human-centric approach to building a smarter and better parking application. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 514-519). IEEE.

Liu, C., Li, J., & Zhang, D. (2024). Fuzzy Fault Tree Analysis and Safety Countermeasures for Coal Mine Ground Gas Transportation System. Processes, 12(2), 344.

Lteif, G. (2024, March 24). Part 5: High-level solution design (HLD) documents: What is it and when do you need one. SoftwareDominos.

Madni, A. M., & Sievers, M. (2018). Model-based systems engineering: Motivation, current status, and research opportunities. *Systems Engineering*, *21*(3), 172-190.

Mangiaracina, R., Tumino, A., Miragliotta, G., Salvadori, G., & Perego, A. (2017, September). Smart parking management in a smart city: Costs and benefits. In 2017 IEEE international conference on service operations and logistics, and informatics (SOLI) (pp. 27-32). IEEE.

Marcellin, M. C., Pavur, G., Loose, D. C., Cardenas, J. J., Denehy, D., Almashhadani, M., ... & Lambert, J. H. (2023). Risk Model of Climate Change and Water Scarcity for Energy Resources of Iraq.

Marcellin, M. C., Pavur, G., Loose, D. C., Cardenas, J. J., Denehy, D., Almashhadani, M., ... & Lambert, J. H. (2024). Systems analysis for energy assets of Iraq influenced by water scarcity. *Environment Systems and Decisions*, 1-21.

McGregor, J., Cohen S.G. (2022, November 21) Modeling Languages for Model-Based Systems Engineering (MBSE). Retrieved June 19, 2024, from https://insights.sei.cmu.edu/blog/modeling-languages-for-model-based-systems-engineering-mbse/.

Mhenni, F., Nguyen, N., & Choley, J. Y. (2016). SafeSysE: A safety analysis integration in systems engineering approach. *IEEE Systems Journal*, *12*(1), 161-172.

Mifra Electronics. (2024, February 22). Smart car parking system project. Retrieved from https://mifraelectronics.com/smart-car-parking-system/

MITRE Corporation (2014) MITRE Systems Engineering Guide

Moghadasi, N., Collier, Z.A., Koch, A., Slutzky, D.L., Polmateer, T.L., Manasco, M.C., & Lambert, J.H. (2022). Trust and security of electric vehicle-to-grid systems and hardware supply chains. *Reliability Engineering & System Safety, 225*, 108565. https://doi.org/10.1016/j.ress.2022.108565

Moghadasi, N., Piran, M., Baek, S., Valdez, R. S., Porter, M. D., Johnson, D., & Lambert, J. H. (2023, December). Systems Analysis of Bias and Risk in AI-Enabled Medical Diagnosis. In *2023 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1800-1807). IEEE.

Moriarty, K. Kvien, A. (2021) U.S. Airport Infrastructure and Sustainable Aviation Fuel *National Renewable Energy Laboratory*

Nakao, H., Katahira, M., Miyamoto, Y., & Leveson, N. (2011, October). Safety guided design of crew return vehicle in concept design phase using STAMP/STPA. In Proc. of the 5: th IAASS Conference (pp. 497-501).

OMG Systems Modeling Language (OMG SysML), (June 2010) OMG Specification Version 1.2

OMG, 2018. What is SysML? http://www.omgsysml.org/what-is-sysml.html

Ouhammou, I., Chafiq, T., & Hmamou, M. (2023). IoT-Enabled Smart Parking: Enhancing Efficiency and Sustainability in Smart Cities. In *E3S Web of Conferences* (Vol. 418, p. 02006). EDP Sciences.

Papp Mobility. (2023, October 8). How do IoT parking sensors reduce CO2 emissions?. Retrieved from https://www.pappmobility.com/post/how-do-iot-parking-sensors-reduce-co2-emissions

Paradox Engineering. (2024, May 21). *4+1 benefits of smart truck parking*. Retrieved from https://www.pdxeng.ch/heavy-goods-vehicles/benefits-of-smart-truck-parking/

PATHAK, I., & Kothari, B. (2024). ISO 26262 Functional Safety–An Approach for Compliance Readiness (No. 2024-26-0104). SAE Technical Paper.

Patou, F., Dimaki, M., Maier, A., Svendsen, W.E., & Madsen, J. (2018) Model-based system engineering for life sciences instrumentation development.

Press, D. (2018). Guidelines for failure modes and effects analysis for medical devices.

Provan, D. J., Woods, D. D., Dekker, S. W., & Rae, A. J. (2020). Safety II professionals: How resilience engineering can transform safety practice. Reliability Engineering & System Safety, 195, 106740.

Quante, G., Bullerdiek, N., Bube, S., Neuling, U., & Kaltschmitt, M. (2023). Renewable fuel options for aviation – A system-wide comparison of drop-in and non-drop-in fuel options. Fuel, 333, 126269. https://doi.org/10.1016/j.fuel.2022.126269

Rehena, Z., Mondal, M. A., & Janssen, M. (2018, May). A multiple-criteria algorithm for smart parking: making fair and preferred parking reservations in smart cities. In *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age* (pp. 1-9).

Risk Management (glossary) - SEBoK. (n.d.). Retrieved [date you accessed the page], from https://sebokwiki.org/wiki/Risk_Management_(glossary)

Rodriguez, H. (2023). *Sustainable Aviation Fuel Implementation Strategies for European Airports* (Master's thesis).

Rosenkranz, E. (2021, February 16). Smart parking: How it works & successful examples. Smart CRE. https://smart-cre.com/smart-parking-definition-and-examples/

Shevchenko, N. (2020, December 21). An Introduction to Model-Based Systems Engineering (MBSE)

Stoneburner, G., A. Goguen, and A. Feringa, July 2002, Risk Management Guide for Information Technology System, National Institute of Standards and Technology, Special Publication 800-30, p. 1.

Systems Engineering Body of Knowledge (SEBoK). (2023, November 20). Requirement (glossary). In SEBoK (v.2.9). Retrieved from https://sebokwiki.org/wiki/Requirement_(glossary)

Tran, V. N., Tran, L. V., & Tran, V. N. (2021, March). Functional Hazard Analysis for Engineering Safe Software Requirements. In *2021 4th International Conference on Information and Computer Technologies (ICICT)* (pp. 142-148). IEEE.
United States. (2023). H.R.6271 - Farm to Fly Act of 2023. 118th Congress. Retrieved from https://www.congress.gov/bill/118th-congress/house-bill/6271/text?s=1&r=8

U.S. Department of Energy (2022) SAF Grand Challenge Roadmap: Flight Plan for Sustainable Aviation Fuel

U.S. Department of Energy (2022) Aviation Fuel data Center Sustainable Aviation Fuel https://afdc.energy.gov/fuels/sustainable-aviation-fuel

U.S Treasury Department and Internal Revenue Service (2022) Sustainable Aviation Fuel Credit; Lifecycle Greenhouse Gas Emissions Reduction Percentage and Certification of Sustainability Requirements Related to the Clean Air Act; Safe Harbors

Vincoli, J. W. (2024). Basic guide to system safety. John Wiley & Sons.

Walker, A. (2020). Guest editorial: Johnson Matthey technology review special edition on clean mobility. Johnson Matthey Technology Review, 64(3), 234-235.

Wan, Z., Qin, J., & Wei, Z. (2023). Overview of technical research on safety monitoring, early warning, and risk assessment for underground structural engineering construction. *Emergency Management Science and Technology*, *3*(1).

Weaver, P. (2008). *The meaning of risk in an uncertain world.* Paper presented at PMI Global Congress 2008—EMEA, St. Julian's, Malta. Newtown Square, PA: Project Management Institute.

Wijayaningtyas, M., Ilmi, N., & Winanda, L. A. R. (2024). Occupational Health and Safety Risk Analysis with The Fault Tree Analysis Method. In E3S Web of Conferences (Vol. 476, p. 01061). EDP Sciences.

Wymore, A. Wayne. 1993. Model-Based Systems Engineering: An Introduction to the Mathematical Theory of Discrete Systems and to the Tricotyledon Theory of System Design. Boca Raton: CRC Press

Xin, S., Wang, Y., Wang, L., & Wang, X. (2023). A safety assessment approach of the salvage based on salvor–cable–wreck coupled simulations. *Ocean Engineering*, *269*, 113537.

Yang, Jie, Jinbao He, and Xiongwei Wang. "Design of Intelligent Parking System Based on Internet of Things and Cloud Platform." International Journal of Grid & High Performance Computing 15.2 (2023).

Zhang, Y., Dong, C., Guo, W., Dai, J., & Zhao, Z. (2022). Systems theoretic accident model and process (STAMP): A literature review. *Safety science*, *152*, 105596.

Zhu, Y., Ye, X., Chen, J., Yan, X., & Wang, T. (2020). Impact of cruising for parking on travel time of traffic flow. *Sustainability*, *12*(8), 3079.

Zuken Inc. (n.d.). Requirements traceability in an MBSE environment. Retrieved June 3, 2024, from https://www.zuken.com/us/blog/requirements-traceability-in-an-mbse-environment/

Zulfiqar, H., Ul Haque, H. M., Tariq, F., & Khan, R. M. (2023). A survey on smart parking systems in urban cities. Concurrency and Computation: Practice and Experience, 35(15), e6511.